Soft Target Hardening

Protecting People from Attack

Dr. Jennifer Hesterman
Colonel, U.S. Air Force (Retired)

CRC Press
Taylor & Francis Group

Soft Target Hardening

Protecting People from Attack

Soft Target Hardening

Protecting People from Attack

Dr. Jennifer Hesterman
Colonel, U.S. Air Force (Retired)

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2015 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20141027

International Standard Book Number-13: 978-1-4822-4422-9 (eBook - PDF)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Contents

	Foreword	xiii
	Preface	xv
	Acknowledgments	xix
	The Author	xxi
Chapter 1	Soft Targets	1
	Introduction	1
	The Difference in Threat, Vulnerability, and Risk	6
	References	8
Chapter 2	The Psychology of Soft Targeting and Our Unique Vulnerability	9
	Introduction	9
	What Is Terrorism?	10
	Who Becomes a Terrorist?	10
	Terrorist Motivations	11
	Terrorist Behavior	12
	Terrorism's Effectiveness	13
	Terrorism's Target	15
	Soft Target Violence: A Collective Twenty-First Century Black Swan	16
	The Internet as a Tool	18
	Soft Targeting Motivations	19
	Our Unique Vulnerability	21
	What Do We Most Fear?	22
	How Should We Respond?	24
	References	25

Chapter 3 International Terror Groups: Propensity and Ability to Mount Soft Target Attacks 27
Introduction 27
Modern Terrorism's Roots 27
AQ and Affiliates 29
The Ideology 30
Rise of bin Laden and al-Qaeda 31
Emergent al-Qaeda 32
AQAP 32
Other AQ Splinter Groups 33
Bin Laden Speaks 38
AQ's New Goals and Tactics 38
Hezbollah 39
Methodology and Objectives 40
Primary Area of Operations 40
Tactical Proficiency 40
Active and Deadly 40
Operations in the Western Hemisphere 41
South America 41
Canada 42
At the Mexican Border 43
United States 46
Hamas 47
Hamas in the Western Hemisphere 48
Summary of Threat 49
References 49
Chapter 4 Domestic Terrorism and the Homegrown Threat 53
Introduction 53
History of Domestic Terrorism in the United States 54
The Twenty-First Century and the Rising Tide of Domestic Extremism 58
Right-Wing Extremism 61
Militias 62

Sovereign Citizens 63
Left Wing 66
Anarchists 66
Anarchism and the Military 69
Single-Issue or Special-Interest Terrorism 70
The Earth Liberation Front 70
Animal Liberation Front 72
Homegrown Terror 73
Rehabilitation and the Domestic Terrorist 76
Jihadist Defined 77
Recidivism 78
Counter-Radicalization Efforts 78
Inside the Saudi Program 79
Possible Solutions in the United States 80
The Lone Wolf 82
Mexican Cartels Cross the Border 84
Ideology: Money 85
Tactic: Brutal Violence Against Soft Targets 86
Goals: Money, Power, Control 87
Major DTOs Impacting the United States 88
Special Concern: Los Zetas 89
Zetas Tactics 89
Increasing Reach in the United States 90
Nexus with Gangs 91
Summary of Domestic Terrorist Threats against Soft Targets 92
References 92

Chapter 5 **Soft Target Threat Assessment: Schools, Churches, and Hospitals** 97
Introduction 97
Vulnerability in the United States 98
Small Cities and Rural Areas in the Crosshairs 99
How Bad Actors Choose Targets 100

The Soft Targets 101
Schools 102
K–12 in the Crosshairs 103
K–12 Vulnerability 111
Colleges: Campus Culture and Vulnerability 113
Campuses Already Under Attack 114
Escalating Number of Attacks on College Campuses 117
Bad Blood: Intelligence, Law Enforcement, and Higher Education 118
Churches 121
The Proliferation of Church Attacks 123
US Churches as Targets 124
Hospitals 126
Nefarious Use of Ambulances 129
References 131

Chapter 6 Soft Target Threat Assessment: Malls, Sporting Events, and Recreational Venues 135
Introduction 135
Shopping Malls 136
Other Significant Mall Attacks 141
Terrorist Threats Against US Malls 141
Vulnerable Open Air Marketplaces 142
Sports Venues 143
Stadiums and Arenas in the Crosshairs 143
Performing Arts and Recreation Venues 153
Tourist Sites: A Vulnerable Target 155
References 155

Chapter 7 Hardening Tactics at Global Hotspots 159
Introduction 159
Soft Target Hardening in the Middle East 161
Life in a Compound 162
Schools and Christian Churches 165

Hotel Security 165
The Westerner as a Target 170
State Department Engagement 171
United Nations and Soft Targets 173
References 174

Chapter 8 Soft Target Hardening 101 175
Introduction 175
Steady-State and Crisis Leadership 176
Intuition 180
Insider Threat: A Fifth Column 181
Good Hiring Practices—First Line of Defense 182
Background Checks 183
Kidnapping and the Use of Human Shields in Terrorist Operations 186
Surrounded by Crises 188
First Response and the Threat of Secondary Attacks 189
Weapons of Mass Destruction 190
In the SIRA Method 193
Suicide Terrorism 194
Face of Rage 196
References 199

Chapter 9 Deterring and Mitigating Attack 201
Introduction 201
Effects-Based Hardening (EBH) 202
Physical Security 204
Parking Lots 207
Pre-positioned Vehicle 207
Traffic Duty 209
Security 209
Locks 210
Alarms 212
Visitor Access and Badges 214

Closed Circuit Television (CCTV) 214
Public Address System 215
Ventilation System 216
Dining Halls 217
Emergency Preparations 217
Hold Room 218
Emergency Response Team and the Command Center 218
Bomb Threat 221
Medical Program 221
Shelter in Place 223
Elementary Schools in Focus 224
Hardening the College Campus 225
Building Relationships 225
Students and Staff as Force Multipliers 227
Exercising Due Diligence 227
Churches 228
Hospitals 229
Malls 230
Sports and Recreation Venues 232
Red Teaming Soft Targets 234
Conclusion 235
References 235

Chapter 10 Fifteen Takeaways about Soft Target Hardening 239
Reference 241

Glossary 243

Appendix A: List of Foreign Terrorist Organizations 247

Appendix B: NIMS, the ICS and FEMA Courses 253

Appendix C: Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment Checklist 257

Appendix D: Bomb Threat Checklist 269

Appendix E: National Counterterrorism Center Bomb Threat Standoff Charts 271

Appendix F: Planning and Emergency Smartphone Applications 275

Appendix G: Primary and Secondary School Threat Assessment and Response Checklist 277

Foreword

On August 5, 2012, a White Supremacist killed six people and wounded four others at a Sikh temple in Oak Creek, Wisconsin. On April 15, 2013 two brothers detonated two pressure cooker bombs during the Boston Marathon, killing 3 people and injuring some 264 others. On December 29, 2013, a female suicide bomber killed at least 15 people and injured over 40 at the train station in the southern Russian city of Volgograd. On May 24, 2014, a gunman opened fire at the Jewish Museum of Belgium, in Brussels, killing four people. While these four attacks took place on different continents and were conducted by individuals with different motivations, agendas, tactics, and weapons, they nonetheless shared one characteristic, with all four directed against what are termed "soft" targets—targets that lack robust security, and, therefore, are accessible to the perpetrators. Soft targets, as a result, are, in relative terms, much less difficult to access and attack than their counterpart "hard" targets, which take numerous measures to deter potential attacks by adopting a strong security posture.

As the author of this important book points out, terrorists remain fixated on continuously attacking iconic "trophy" targets. As evidenced by al-Qaeda's horrifically and catastrophically successful aerial destruction of New York City's World Trade Center's twin towers on 9/11 by hijacking multiple airliners, terrorists—especially as small cells or lone wolf operatives who lack the capability to attack hardened targets—keep seeking other softer targets to attack. This includes, though is not limited to, schools and universities, shopping malls, hospitals, hotels, restaurants, sports stadiums and amusement parks, and religious institutions. When attacked, these targets too are sufficiently lethal in their destruction of lives and damage to physical facilities to generate widespread publicity for their various causes (however unjust and illegitimate).

Although, as Dr. Hesterman articulates, it is virtually impossible to protect every potential target, another of this book's significant contributions is its assessment of the factors that might make a target "soft" to its intended attacker and the threat and vulnerability risk assessment methodologies and techniques that need to be adopted by security and

facility managers to harden them. These include the protective measures that need to be implemented during the course of an attack, during the short period of time before law enforcement and emergency first responders are able to arrive at the scene of the incident.

The author's background as a retired Colonel in the U.S. Air Force who had commanded emergency response forces and her extensive experience in counterterrorism give this book an invaluable practitioner's approach that will greatly benefit its readers.

Joshua Sinai, Ph.D.
Senior Consultant on Threat Mitigation, Security Risk, Inc.

Preface

Around the world, battlefield lines have been redrawn to include churches, schools, hospitals, shopping venues, and sporting and recreational events. In some cases, countries are shelling their own towns and citizens to quell uprisings and turn the tide of civil war. Civilian fatalities in conflicts have climbed from 5 percent at the turn of the century to more than 90 percent in modern-day wars. And every day there is a soft target terrorist attack somewhere in the world with innocent men, women, and children caught in the crossfire. This breach of moral boundaries is shocking and causes a ripple effect of fear, two primary goals of terrorist groups.

In military operations, we do everything possible to spare innocent victims from the violence. If the world's "most wanted" terrorist is visiting his child in school or receiving medical treatment at a hospital and we have positive identification plus a clear shot, we will not fire. We believe in and adhere to the Geneva Conventions that protect noncombatants. And we hope our adversaries would similarly respect civilian zones, especially those filled with worshippers, schoolchildren, or patients seeking care. However, as we have further hardened targets such as government buildings and mass transportation, terrorists are turning their sights elsewhere—toward easy-to-access, vulnerable places and people. We have a severe blind spot that our soft targets at home are somehow off limits to those who wish to do us harm. But we are wrong.

This is a topic that must be discussed, a book that had to be written. While collecting data and sources, I realized the importance of being as close to the scene as possible to grasp the event, the response, and the aftermath, so spent hundreds of hours reading eyewitness accounts and viewing video and pictures from horrific soft target terrorist attacks. I watched shoppers at the Westgate Mall doing all of the wrong things during the shooting—like choosing to hide instead of run when they had the chance, wrongly guessing the attack would only last a few minutes. The military and police activity outside the mall was uncoordinated and chaotic, and they even mistakenly fired on each other during hostage rescues. At the Beslan school siege, there was no cordon around the scene,

and angry parents were permitted to bring their firearms to supplement the police and the military. Responding forces were unprepared to handle situations such as the use of white-flag-waving human shields by the terrorists. At the Moscow Dubrovka Theater, the Russian government killed innocent hostages by pumping a lethal amount of gas into the theater to bring the three-day siege to closure and then choosing not to tell responding medics the type of agent, meaning no antidote and 130 civilian choking deaths.

As a military officer, I was the incident commander for hundreds of emergencies, including motorcycle fatalities, car accidents, aircraft incidents, domestic and hostage situations, fuel spills, suspicious packages, chlorine gas leaks, and building fires. A military base is like a small town, a hard target filled with soft targets including dormitories, cafeterias, schools, daycare centers, grocery and department stores, and housing developments, which complicated security and emergency response efforts. The US model encouraging families to coexist on base with a combat mission is not the same as those used by other countries, especially in the Middle East. After visiting some of these overseas installations, I now see the wisdom in the base being treated as a workplace instead of a small town. Certainly, the colocation of hard and soft targets can be disastrous, as we learned in the April 1995 bombing of the Alfred P. Murrah Federal Building in downtown Oklahoma City, when nineteen innocent daycare children were lost at the hands of a domestic terrorist who saw them as "collateral damage."

Despite the lesson that might have been taken from the OKC attack, the Pentagon daycare center remained open, just yards from the main building. On 9/11, the now-closed center was thankfully on the opposite side of the building from the impact area, although it suffered from the smoke plume and was an additional concern for first responders at the scene. Fourteen years later, we might consider the daycare center itself as a primary target. This example illustrates how modern terror events are unforeseen, unplanned, and asymmetric, often forcing us to hit the "reset" button on how we live, work, and play. Perhaps it is human nature to think we have seen and imagined it all but there will be future attacks that will again leave us shaking our heads in disbelief.

There are many approaches to the soft target attacks topic; the tactician will ask how the actors attacked, and the social psychologist will ask why. I discovered that both are equally important to understanding the soft targeting phenomenon, thus both are covered in this book. In the soft targeting realm, there are two types of actors: the opportunist, who usually is acting out of rage and chooses a target and attacks; and the planner, who methodically prepares. The good news is that soft target hardening will repel and mitigate all types of actors, from criminals to insiders. It will also make your building occupants and customers feel

safer and empowered, allowing them to have a more enriching experience whether at school, church, medical appointments, shopping, or relaxing at a sporting or recreational event. This book harnesses over 275 sources with case studies, best practices, and methodology for identifying vulnerabilities and mitigating risk.

As with all change, there is resistance, especially when we feel that altering our way of life is conceding victory to adversaries. But the world has changed, and so must we. I currently live in the Middle East and now understand the importance and methodology of lowered profiles and robust fortification to protect civilians. For example, in the twisting, compressed chaos of the souq, I can spot an American tourist a mile away—not only by dress, but also by mannerism, voice, and details such as sunglasses and jewelry. However, American residents learn to blend into the fabric of society; we must in order to feel comfortable moving about and living in an unstable region. On the physical security side, the "compound mentality" makes sense on many levels, and we enjoy this extra barrier of security where we live, work, and play. I added this unique perspective of living in the Middle East to the book—not implying the methods are superior, but to add a few extra ideas for the security toolbox.

If you take one thing away from this book, it should be that we are not helpless in these uncertain times. Ignoring the rising tide of soft target terror in the world and hoping it won't cross our borders is not a sound strategy. Understanding the threat, assessing vulnerability, and taking measures to lower risk is the pathway to deterrence and mitigation; this book provides those tools.

Acknowledgments

Of course, this work would not have been possible without the support of many. First, special thanks to Sarah Kinzer, Brian Gallagher, Ralph Fisk, and Eileen Jorns for their valuable insight and assistance with the project. Thank you to John DiGennaro, for the support and encouragement while I finished my dissertation and doctoral program, and Oz Morales, for keeping the military side of things together while I spent thousands of hours at the computer. On the work front, thanks to Alex Anyse and Tae Kim at the MASY Group and to the editor of the *Counter Terrorist Magazine,* Chris Graham, for their friendship and ongoing support of my myriad endeavors. Also, I owe a large debt of gratitude to my patient and extraordinary editors at Taylor & Francis/CRC Press: Mark Listewnik, who entrusted me with this special topic; and Jennifer Abbott, Suzanne Lassandro, and Stephanie Morkert, who took this project from rough manuscript to professional publication.

I would like to give special appreciation to my family for their love and support. My parents, Lloyd and Barbara Whitnack, bestowed both a great work ethic and the belief that anything is possible. Thank you to my brother, Matt Whitnack, for a lifetime of friendship. Much appreciation and love to my wonderful family—husband, John, and daughter, Sarah—for always supporting my dreams. Finally, thanks to my office companion and good-natured Labrador retriever, Hunter, for knowing when I needed a little fresh air and TLC.

You all inspire me to be a better person and to live each day richly and without regret.

The Author

Dr. Jennifer Hesterman, U.S. Air Force (retired), was commissioned in 1986 as a graduate of Air Force ROTC at Penn State University. During her military career she served in three Pentagon tours, commanded both logistics support and mission support squadrons, and served as a mission support group commander. Her last assignment was vice commander, 316th Wing, at Andrews Air Force Base, Maryland, the home of Air Force One. She was responsible for installation security, force support, and the 1st Helicopter Squadron, and regularly greeted the president and other heads of state on the ramp. Her decorations include the Legion of Merit and the Meritorious Service Medal with five oak leaf clusters.

Dr. Hesterman has a doctoral degree from Benedictine University and also holds master's degrees from Johns Hopkins University and Air University. In 2003, she was a National Defense fellow at the Center for Strategic and International Studies in Washington, DC, where she immersed herself in a year-long study of the nexus between organized crime and international terrorism. She is also a 2006 alumna of the

Harvard Senior Executive Fellows Program. A cleared professional, Dr. Hesterman is an advisor for Watermark Risk Management International, a senior analyst for the MASY Group, on the Advisory Board for the Government Security Conference, and a member of the ASIS Crime and Loss Prevention Council. She is a contributing editor for the *Counter Terrorist Magazine* and author of *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime and Terror Groups* (CRC Press 2013). She lives in an undisclosed location in the Middle East.

CHAPTER 1

Soft Targets

> 10 hours have passed and the Mujahideen are still strong inside #Westgate Mall and still holding their ground. All praise is due to Allah!
>
> **—Al-Shabaab tweet, September 21, 2013**

INTRODUCTION

The Westgate Mall in Nairobi, Kenya, was a new, Israeli-owned, upscale shopping facility frequented by US and Canadian embassy personnel, expatriates, and locals for its great food, shopping, and entertainment. In addition to a large children's play area, the mall boasted a mid-sized casino that served alcohol to high-stakes gamblers. Westgate and its unsuspecting occupants were a perfect target for al-Shabaab terrorists, who attacked on Saturday, September 21, 2013, killing 67 people and injuring 179 others in a four-day standoff. The fears of intelligence and security analysts around the world were realized: shopping malls were officially added to the terrorist playbook.

In the post-9/11 world, the United States has made great strides to further reinforce already hardened targets such as military installations, government buildings, and transportation systems. Those facilities now employ concentric rings of security, more cameras, and increased security manpower, serving to repel would-be terrorists and violent criminals. However, as these hard targets are further reinforced with new technology and tactics, soft civilian-centric targets such as the Westgate Mall are of increasing interest to terrorists. But this concept is not new; although lost in the news at the time, evidence collected following the 9/11 attack proved the aircraft hijackers also accomplished preliminary planning against soft targets, surveying and sketching at least five sites including Walt Disney World, Disneyland, the Mall of America, the Sears Tower, and unspecified sports facilities (Merzer, Savino, and Murphy 2001). Despite horrific terrorist operations against civilians such as the 2002 Beslan school massacre, the 2005 Moscow theater siege, the

2008 Mumbai attacks, and the 2013 Nairobi shopping mall assault, few resources have been applied toward hardening similar soft targets in the United States. A very small portion of our national security budget and effort is spent protecting civilian venues. Responsibility for security is often passed on to owners and operators, who have no training and few resources. In military terms, we are leaving our flank exposed.

The problem is far more complex than a simple lack of funding; the challenges are also psychological and tactical. First of all, contemporary terrorism has no moral boundaries. Who could have predicted, even ten years ago, that schools, churches, and hospitals would be considered routine, legitimate targets for terrorist groups? Outrage and outcry at the beginning of this soft targeting era has given way to acceptance. Psychologically it is more comfortable to pretend there is no threat here in the homeland, that these heinous attacks will always happen "somewhere else." Americans also have a very short memory—a blessing when it comes to resiliency and bouncing back from events like devastating civil and world wars, the Great Depression, and 9/11. However, in terms of security, this short-term memory can be our Achilles heel when faced with a determined, patient enemy. In fact, we almost have a revisionist history, downplaying and explaining away previous attacks as individual acts of violence by groups of madmen, not seeing the larger trends.

We have a tendency to hide behind numbers; the number of violent crimes committed in our country is down, which makes us feel good about our security efforts. However, the scale of violence and deaths resulting from those crimes appears to be rising, an underlying trend that is far more important. Some facility owners and managers choose to roll the dice, sacrificing a robust security posture to provide a more pleasant experience for students, worshippers, shoppers, or sporting or recreational event fans. We must remember that the choice of target for terrorists is not random, particularly for radical religious groups that want elevated body counts, press coverage, and a fearful populace in order to further their goals. Hardened targets repel bad actors, and unprotected soft targets invite.

Attacks against soft targets have a powerful effect on the psyche of the populace. Modern terrorist groups and actors have redrawn the battlefield lines, and places where civilians once felt secure have been pulled into the war zone. Persistent, lethal attacks by al-Qaeda-affiliated terrorists against churches, hospitals, and schools in the Middle East and Africa have even successfully shifted the center of gravity in major conflicts. When places formerly considered "safe" become targets, frightened civilians lose the will to fight. They may flee and surrender the territory to the aggressor or rise up en masse, compelling the government to make concessions to insurgents to stop the brutality against noncombatants.

Due to our country's adherence to the Geneva Conventions, we will not attack soft targets with no military necessity, even if the enemy takes shelter among the people. Civilians are not treated as combatants and therefore are not targets. Injured civilians are protected, not fired upon. Places of worship are never purposely hit. Schoolyards filled with children are not a target. We are intellectually unwilling to imagine an enemy who does not share what we believe to be universally accepted moral codes; therefore, we have a severe blind spot and are wholly unprepared to protect soft targets in our country. We must understand that our enemies see a busload of children and a church full of people as legitimate targets. Terrorists do not care about "collateral damage," a phrase Timothy McVeigh unremorsefully used to describe the daycare children killed in his attack at the Alfred Murrah Building. We also tend to forget that domestic terrorists have routinely hit soft targets in our country, from arson to shooting, and bombings. And, no matter your gender, race, religion, or sexual preference, there is a hate group in the United States actively or passively targeting you. Therefore, we must prepare both psychologically and tactically to harden our soft targets and lessen their vulnerability.

Protecting soft targets presents unique challenges for law enforcement because the buildings are privately owned and responsibility rests on the owners to secure the property and its occupants. Therefore, partnering is critical: educating the owners on the threat, assisting with vulnerability assessments, and helping to harden the venue or establishment. However, when I speak with college presidents, high school principals, clergy, or owners of soft target venues about the possibility of a terrorist attack on their property, they may convey a feeling of *hopelessness* (there is not much we can do to prevent or mitigate the threat), *infallibility* (it will never happen here), or *inescapability* (it is destiny or unavoidable, so why even try). Those who frequent soft target facilities—employees and patrons alike—typically believe that "It can't happen to me." They have a sense of *invulnerability*. Even worse, others may believe that "If it is going to happen, there is nothing I can do about it anyway," expressing *inevitability*. People with these mindsets are a detriment in an emergency situation, with no awareness of the threat, mental preparation, or sense of determination to engage during the situation. In an emergency, those without a plan or resolve may wait for first responders and law enforcement to arrive and rescue them before taking steps to save their lives and those of others. The Sandy Hook shooting event was over in six minutes, with twenty-six dead: there is no time to wait for help when the attacker is determined and brings heavy firepower to the fight. You are the first responder.

Most experts agree that, with our newly robust intelligence capabilities, another coordinated mass casualty event in multiple locations

such as the 9/11 attacks is unlikely. However, the threat of a Mumbai-styled event in a city with multiple avenues of approach (water and land) or a mass casualty bombing at a soft target location is more probable and will have an associated shock factor. There is a general hesitation for the government to share specific threat information with the public, perhaps because we do not want to cause panic; however, education is the best way to lower fear, as people will feel they can protect themselves and their loved ones. As witnessed in several natural disaster events in our country since 9/11, citizens are generally overly reliant on the government, lacking supplies at home as simple as flashlights, radios, batteries, nonperishable food, and water. Unfortunately, many police departments and hospitals have taken large funding cuts due to our country's financial crisis, meaning response time may be slower than anticipated. During mass casualty events such as shootings or a fire, victims routinely are unable to locate emergency exits and they have no plan to defend themselves and others. Furthermore, most people do not understand what it means to "shelter in place" or how to follow other orders that may be given during a serious emergency. The combination of lack of education about the threat, a feeling of invulnerability regarding soft target attacks, over-reliance on the government for help, and lack of first-response resources is potentially disastrous. Citizens must be educated on the threat and response and become valuable force multipliers instead of adding to challenges at the scene.

Security training and resources are typically the first to go during budget-cutting drills. When leaders are faced with a budgeting dilemma, a good question might be: "What is the cost for not protecting our people?" Certainly, most schools, churches, and hospitals are not flush with cash and find it difficult to spend valuable dollars on security. Often, decisions are arbitrarily made instead of using a system to assess vulnerability and threat, and then obtain the right mitigation tools to lower risk and protect the unique venue. With regard to profit-making soft targets such as malls and sporting and recreational venues, there is a desire for balance between security and convenience minimizing the impact to the customer. Business owners see customer backlash when other facilities add layers of active, hands-on security; it likely discourages them from pursuing similar activities. For example, the addition of backscatter technology at airports drew the ire and scrutiny of millions of people, many of whom did not even fly on a regular basis. Even news of the almost-catastrophes in flight with shoe and underwear bombs did little to persuade the public for the necessity for the systems. Security may not be popular and decisions should not be made by consent.

If businesses are concerned about their reputation for long security lines and visitor frustration, owners should consider the damage to their reputation should a mass casualty terrorist or violent criminal

attack happen on their property. For instance, the movie industry as a whole was impacted by the shootings at the Cinemark Theater in Aurora, Colorado, on July 20, 2012, at the premiere of the movie *The Dark Knight Rises*. In response to the violent attack, the film's producer, Warner Brothers Studios, pulled that movie and all of its violent movies from theaters. As attendance dropped dramatically worldwide, theater owners paid extra for increased security to reassure their customers. Cinemark not only paid for the burial expenses of the twelve victims, but also gave each family $220,000. The company was able to avoid paying millions of dollars of hospital bills for the seventy injured theatergoers, as they were forgiven and funded by the state. However, despite these actions, Cinemark was still sued by the families for not preventing the event, with decisions pending.

The lavish Westgate Mall, which was portrayed as a symbol of Kenya's future and cost hundreds of millions of dollars to build, had high-end stores and affluent customers who generated millions of dollars in revenue weekly. The mall was completely destroyed in the four-day siege with al-Shabaab terrorists, and only half of the store owners had terrorism insurance (Vogt 2014). Stores were looted during and after the event by corrupt soldiers, adding to the financial ruin of shop owners. Rebuilding the mall is a must to show resilience and national pride; however, the cost is exorbitant for the country and insurers. Also, the inability of mall personnel to detect the planning stages of the attack, the ineffective response by armed mall security to put down the offensive, and the lack of communication with shoppers and store owners inside the mall about the unfolding events have been widely criticized. The downplaying of the severity of the situation by the government and its sluggish, uncoordinated response cast doubt on its ability to handle violent events in the country. The tourism industry, critical to Kenya's fragile economy, was hit hard, with 20 percent fewer visitors in the months following the attack, and hopes for hosting future Olympic games and World Cup soccer events dashed. Lax security at one mall sent devastating ripples through an entire national economy and harmed future prospects for development.

Although international terror remains a viable threat to our country, domestic terrorism from right-wing, left-wing, and single-issue groups is perhaps a greater daily concern for our law enforcement agencies. The growing propensity of these organizations and their members to "act out" on soft targets and to step up and engage law enforcement is alarming. The radicalization of Americans continues, with several successful attacks by homegrown jihadists and more than sixty more thwarted since 9/11. Exacerbating the threat, the lack of a rehabilitation program means there is no way of ensuring those who serve their prison sentence and return to society will not go back to their old terroristic ways

… with a vengeance. Furthermore, the threat of the lone wolf, already embedded in society and acting alone with unyielding determination, is extremely worrisome. Factor in an unprecedented increase in hate groups and gangs in our country, and the domestic terrorism picture becomes quite grim, with resource-constrained law enforcement agencies struggling to juggle myriad challenges. Finally, brutal Mexican drug trafficking organizations are now operating in the United States; cartels are using gangs to move product and corrupting border patrol officers who open lanes and permitting people and drugs (and potentially worse) into our nation. As a paramilitary organization with the tactical knowledge and equipment of a small army, the Los Zetas cartel, now as far north as Chicago, provides the most vexing threat. Cartels use brutal tactics against soft targets in an effort to influence the political process and instill fear in the populace—factors that elevate them beyond mere criminal groups.

This book is the first of its kind to explore the topic of soft targeting. The work studies the psychology of soft target attacks, our blind spots and vulnerabilities, and attributes that make civilian-centric venues appealing to bad actors. Next, looking through the lens of past, current, and emergent activities, the research yields an estimate of the motivations and capabilities of international and domestic terrorist groups, as well as drug trafficking organizations (arguably terrorists), to hit soft targets in our country. A current assessment of soft target attacks worldwide will give insight to trends and operational tactics. Studying the activities of terrorist groups that successfully and repeatedly strike soft targets, such as Chechen extremists, reveals security vulnerabilities and how poor government engagement and response can intensify the number of casualties. Finally, training and tactics for psychological and infrastructure hardening, as well as planning and exercising strategies, provide a road map for those who own, operate, protect, and use soft target locations.

THE DIFFERENCE IN THREAT, VULNERABILITY, AND RISK

A few working definitions will help frame the discussion of soft targeting. The concepts of threat, vulnerability, and risk are routinely intermingled and exchanged; the graphic in Figure 1.1 helps explain the concepts and their relationship.

Examining and understanding our vulnerabilities is the first step to address cultural and personal limitations that keep us from adequately comprehending and addressing soft target threats. Your ability to deter attack is amplified by understanding the threat, and Chapters 3 and 4 analyze the groups and actors mostly likely to strike soft targets. A small

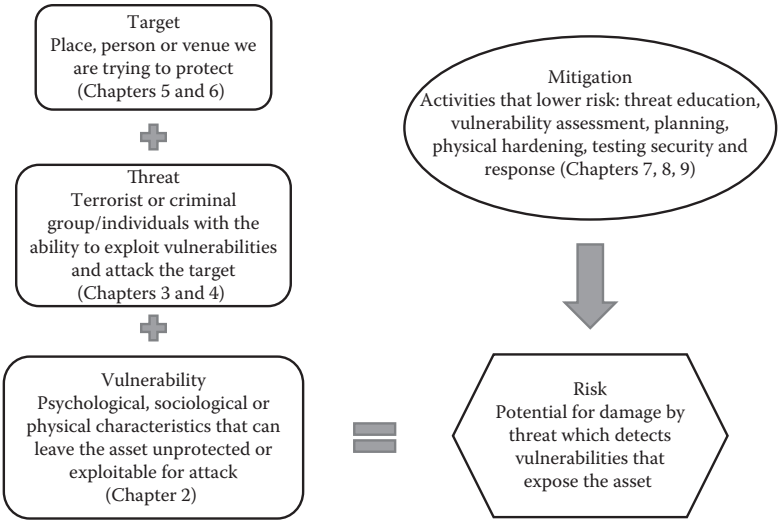

Target
Place, person or venue we are trying to protect (Chapters 5 and 6)
Threat
Terrorist or criminal group/individuals with the ability to exploit vulnerabilities and attack the target (Chapters 3 and 4)
Vulnerability
Psychological, sociological or physical characteristics that can leave the asset unprotected or exploitable for attack (Chapter 2)
Mitigation
Activities that lower risk: threat education, vulnerability assessment, planning, physical hardening, testing security and response (Chapters 7, 8, 9)
Risk
Potential for damage by threat which detects vulnerabilities that expose the asset

FIGURE 1.1 Threat, vulnerability, and risk model.

portion of the material regarding specific terror and cartel threats was adapted from my last book, *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups* (Hesterman 2013), but is updated and expanded upon to include information regarding propensity and capability to strike soft targets. Case studies presented in the book about soft target attacks or attempted attacks give insight on how future attackers may emulate or change tactics to increase their likelihood of success. Typically, after a successful or failed terrorist attack, much of the focus is placed on the "how" of the operation—methodology and tactics used by the perpetrators. Certainly, these data help us harden targets against copycats or other would-be terrorists and are included in the book. However, to harden psychologically, soft targeting science demands that we also spend time on "why," contemplating why bad actors would strike a soft target and the possible gains. This question is addressed throughout the book to enhance understanding of how soft targeting evolved and how we might deter, discourage, and disincentivize actors from striking.

Chapters 5 and 6 assess the targets themselves and their unique venues, users, and environs to provide insight into hardening challenges (and advantages). The final three chapters educate on how soft targets are hardened overseas, basic principles and specific hardening activities, tools, and checklists. This work introduces the concept of effects-based hardening (EBH) as a systematic, effective methodology to apply your resources to lessen vulnerability. Using this process, venue-specific risk may be assessed and effective mitigation efforts sourced and

implemented to better protect your soft targets and their innocent users from attack.

The use of imagination and intuition is critical when addressing soft target threats. Perhaps the most powerful statement in the 9/11 Commission report comes from its Chapter 11, "Foresight—and Hindsight." The investigators cite a lack of *imagination* as a root cause of the two worst attacks in our country's history: Pearl Harbor and 9/11. This book encourages critical thinking about soft targeting; and those entrusted with protecting venues should actively run "what if" scenarios through their minds while reading. Questions might include, "Is it possible my building and its users might be targeted in this manner? What is the one most vulnerable feature; is it access? Location? The users themselves? Our mission?" In addition to this type of brainstorming and soft targeting education, training, and planning activities, I also recommend in Chapter 9 that facility owners accomplish military-style red teaming activities, as well as both tabletop and live exercises. Testing your security and response is the only way to reveal deficiencies in both planning and infrastructure and will build confidence in your ability to handle an attack.

This book is a broad brushstroke regarding the phenomenon of soft targeting and is meant to stimulate thought and start the conversation about vulnerability, threat, and response. It is not merely focused on response to an attack, but the critical front work of detection, prevention, deterrence, and mitigation. By reading this work, you are participating in mental hardening, making you a force multiplier no matter whether a citizen, community leader, principal, clergy, hospital administrator, sports or recreational venue or shopping mall operator, law enforcement, intelligence analyst, or first responder.

Let us get the national dialogue going.

REFERENCES

Hesterman, Jennifer. *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups.* Boca Raton, FL: CRC Press, 2013.

Merzer, Martin, Lenny Savino, and Kevin Murphy. "Terrorists reportedly cased other sites: Sports facilities, Disney World, Disneyland and the Sears Tower were surveyed." *Philadelphia Inquirer,* October 13, 2001.

Vogt, Heidi. "Shaken Kenya Aims to Rebuild Mall and Its Confidence." *Wall Street Journal,* February 28, 2014.

CHAPTER 2

The Psychology of Soft Targeting and Our Unique Vulnerability

> They never killed children. We really didn't expect this because we thought that they might have some values, terrorists might have some code of conduct.
>
> **—Yousafzai Ziauddin, on the shooting of his daughter, Malala (BBC video 2013)**

INTRODUCTION

Even Yousafzai Ziauddin had a blind spot. Living in the Swat Valley on the Afghanistan–Pakistan border, an area where civilians are routinely terrorized by the Taliban, he still encouraged his 15-year-old daughter, Malala, to campaign publicly for education rights for girls. He believed terrorists would not target and kill her. However, on October 9, 2012, Malala's school bus came to a stop and two masked gunman boarded. One directly approached, shooting her in the head point blank in front of her terrified friends. Both men ran from the bus and were never captured. Capitalizing on the fear inflicted on the local populace and knowing they would never face prosecution, the Taliban immediately took credit for the shooting. Thankfully, Malala received lifesaving care in Pakistan and was transferred to a hospital in the United Kingdom for further surgery and rehabilitation. Undaunted by ongoing death threats from the Taliban, she continues to speak out for her cause while attending school in London and was awarded the Nobel Peace Prize in October 2014.

Understanding what motivated the terrorists is important to understanding Malala's story. A senior Talibani, Adnan Rasheed, sent Malala a four-page letter of explanation for the shooting by a lower-level group member. The overarching theme was that students who go to traditional

schools should instead be attending madrassas, Islamic religious schools that often feed radical jihad. So, in the end, it was merely a manpower issue: more children in traditional schools means fewer terrorists on the street. Malala was caught in the middle, and Rasheed even expressed that "It was shocking for me. I wished it would never [have] happened" (DeHart 2013).

WHAT IS TERRORISM?

Terrorism is different from other crimes. Through acts of extreme violence, terrorists seek to advance an agenda, be it political change or religious domination. Terrorism is a crime, but does not lend itself to the same disincentives as normal offenses. The threat of prison or even death does not deter. We also must be careful in our approach to terrorists due to a dangerous paradox: the more brutal and oppressive we are, the more we make them martyrs to be emulated by others (Dershowitz 2002).

Terrorism is a complex phenomenon. There is no one root cause fueling terrorist activity; if so, we could simply fix the issue by addressing the aggravator and dissuade new group formation. Although the "hearts and minds" strategy is important to pursue, focusing solely on factors such as poverty and illiteracy fails to explain why groups with far greater grievances do not resort to terrorism (Dershowitz 2002). The approach also fails to explain why upper-class, educated individuals answer the jihadist call. Of course, we should continue to address perceived root causes of terrorism, but we must continue to study the ambiguity and myriad factors involved in the terrorism phenomenon.

WHO BECOMES A TERRORIST?

The terrorist believes his or her goals are just and that actions taken to further the cause are justifiable. A very black-and-white picture is painted of the "enemy" or those who stand in the way of goal attainment. In the quest for social, religious, or political change, the terrorist lashes out directly either at the perceived opponent or at another target with the intent of bringing attention to the cause.

However, after intense study of modern terrorist activity and having taught psychology of terrorism courses at the university level to first responders and intelligence analysts, I have come to the conclusion that terrorists are very rational actors. There is no conclusive evidence that terrorists are abnormal, psychotic or have personality disorders. Consider that in the last few years, foiled terror plots included rational actors who were educated, middle or upper class, and dedicated to their

jobs and families. Statements from those closest to the terrorist suspect are usually very telling, and they typically indicate no suspicion the person they knew and loved for years would load a Jeep with explosives and park it in Times Square, or fly to an unfamiliar country and detonate a suicide vest. We routinely underestimate the terrorist's intelligence and sophistication—another blind spot.

TERRORIST MOTIVATIONS

What motivates an individual to join a terrorist group? Jessica Stern, a noted Harvard professor and terrorism expert, has interviewed numerous members of terrorist groups. When discussing al-Qaeda, Stern (2003) notes:

> Militants have told me terrorism can become a career as much as a passion. Leaders harness humiliation and anomie and turn them into weapons. Jihad becomes addictive, militants report, and with some individuals or groups—the "professional" terrorists—grievances can evolve into greed: for money, political power, status, or attention.

So the initial powerful "hook" for joining the jihadist movement may give way to other incentives over time.

The area of terrorist motivation is ripe for further exploration. Before taking up the cause, the terrorist group member was influenced somehow. What trigger flipped the switch from "off" to "on" and turned a father, son, daughter, student, or professor into a jihadist? By exploring this central question, we may develop a type of pre-emptive deprogramming operation preventing the spread of the radical Islamist ideology or supplanting a counternarrative, pushing the continuum toward our goals. There are three general schools of thought on what motivates an individual toward group membership, regardless of the type of organization:

(a) Instinct theory: Group membership behavior is a function of a person's instinct, rather than activities that are conscious, purposeful, and rational.
(b) Reinforcement theory: The decision to be part of the group is strongly affected by knowledge of rewards from its past behaviors.
(c) Cognitive theory: Belonging to the group is influenced more by a person's belief and expectations for future rewards, not possible consequences.

Understanding the motivation to join a terrorist group is important for providing the counternarrative to recruiting efforts and to offering alternatives for those susceptible to the message of violence

and hate. Looking at a mature group/corporation such as Hezbollah in total can be overwhelming when it comes to engagement and disruption. However, excavating the group down to the individual members and their motivations could be significant in developing deradicalization tools and dissecting the group from within. In postmodern society, microlevel changes are proving to be much more powerful than those taken at the macrolevel.

TERRORIST BEHAVIOR

Individuals are drawn to certain groups, feeling a unique connection at some level. Perhaps there is a demographic similarity among members such as religious belief or shared collective experience. Individual behavior and traits imprint on the entire group, so with the admission of a new member, the group changes in subtle but perhaps important ways. Group members bring their biographic background (including any "baggage"), abilities, intelligence, expectations, and personality into the organization. In terms of structure and culture, the group has norms, roles for members, and a level of cohesion. Size plays a role in a group's behavior, as well as its composition. In terms of performance, there are several possible outcomes; members are either satisfied or there could be turnover and even desertion.

We tend to act quite helpless when it comes to terrorist groups; however, they are quite easy to understand when viewed through the lens presented before, and we could take significant action to alter their course. For example, we could provide a counternarrative to group members and inject game changers. In fact, every variable and dynamic in a terrorist group could be specifically targeted in order to change the group's overall behavior and course. Viewing a terrorist group through a construct made popular by organizational behavior experts Szilagyi and Wallace is extremely valuable. If we adhere to the theory that terrorist groups have normative behaviors, despite their goals, adapting standard organizational behavior theory from Szilagyi and Wallace (1990) to terrorist behavior yields a new set of truths:

1. Behavior in terrorist groups is caused.
2. Behavior in terrorist groups is purposive and goal directed.
3. Behavior of the terrorist group is learned.
4. Individuals differ, but a terrorist group will have a shared set of values and characteristics.

Therefore, understanding individual and group dynamics could yield new solution sets for protection against soft target attack.

TERRORISM'S EFFECTIVENESS

Everything that makes democracies great makes them vulnerable to this enemy. Terrorism is much more effective against democracies than closed societies such as North Korea and China. For instance, consider the free press. Terrorism is an elaborate marketing campaign, and publicity adds to the legitimacy of the group and furthers its goals of creating fear. Democracies believe in freedom of information, providing the perfect tool for group member motivation, recruitment, and garnering public sympathy. Technology also plays a role, inasmuch as unfiltered news is often generated and distributed within seconds of an event taking place through Twitter, Facebook, and other social media outlets, in addition to traditional news channels. A closed society that controls the press and its "message" would not provide the terrorist organization this type of advantage.

For instance, how could a fundamental change in Western media's reporting of events impact the power of a terrorist group? Greatly, if you consider fear is a desired outcome of these groups' attacks. Consider social psychologist Kurt Lewin's "force field analysis," a system for predicting the motivated behavior of an individual in his or her "life space." Lewin defined the life space as an individual's perceived reality based on the many factors, real and imagined, at play. In terms of the threat of terrorism, it is important to emphasize the word "perceived" for this analysis. For instance, if a man believes he is being followed down a dark alley, this is his perceived reality and whether a pursuer actually exists is irrelevant. The man will suffer physiological changes associated with fear and panic, and his "fight or flight" instinct will involuntarily take over. Factors feed our perceived reality of the threat of terrorism such as press coverage; panic induced by quick spread of false information through social media; and, if the terrorists are savvy enough, a psy ops (psychological operations) campaign to make us believe something that is not true.

Also, closed societies would not exercise restraint when retaliating against terrorist groups and their members, instead taking swift, brutal countermeasures to suppress antigovernment activity. In a democracy, we believe that one is innocent until proven guilty in a court of law. We provide due process and legal representation to even the most heinous bad actors in society and give them a chance to present their case to a jury of their peers for decision. For conviction, the law requires proof beyond reasonable doubt—something difficult to obtain when it comes to the arrest of sleeper cell members and would-be terrorists; if the trigger has not been pulled on an operation, they may receive light sentences and return to society quickly and without mandated rehabilitation.

Consider the case of Jose Padilla, former member of the Latin Kings street gang, al-Qaeda member, and so-called "dirty bomber." He was arrested in 2002 and it took five years for his case to go to trial and another year for sentencing. In non-Democratic countries, a decision would have been rendered quickly with immediate and severe punishment. When a terrorist is identified and detained in our country, innocent family members are not a target for retaliation; however, in other societies, their homes may be razed and they are punished and sometimes killed. Finally, the ease of moving about a democracy undetected is attractive to terrorists. Our country lacks internal checkpoints and is heterogeneous, with a broad demographic base. This allows bad actors to move more easily across our borders and then just disappear into society. In short, our democracy provides fertile ground for terrorists.

Alan Dershowitz, author of *Why Terrorism Works* (2002), proposes that amoral societies would engage in several (arguably successful) ways to stop the terrorist threat. For example, they would

Completely control the media's reporting on terror incidents and, simultaneously, use the media for disinformation operations.
Monitor all citizen communications.
Criminalize "advocacy" of the terrorist group through inciting speech.
Restrict movement within the country with layered identification checkpoints and even segregation of certain demographics within the country.
Carry out collective punishment with family members and even entire villages to dissuade future activities.
Initiate pre-emptive attacks against the group.

Naturally, this does not sound like a course of action that would be taken by the United States due to our protections under the Constitution and innate sense of justice. However, consider the impact any of these activities, taken alone or in total, would have in our fight against terror. Is there a gray area? The events of 9/11 led to enhanced law enforcement activity, such as more extensive surveillance and wiretapping powers under the USAPATRIOT Act. The resulting skepticism was warranted, as we certainly must safeguard our constitutional protections and closely monitor any erosion of our civil liberties because this is a "slippery slope." However, in the asymmetric fight against an unpredictable, dangerous, and adaptable enemy, we may not be able to have it both ways when dealing with modern terrorist groups. We clearly need a corresponding modern and flexible solution set. To summarize, the very ideals constituting a democracy are leveraged and exploited by terrorist groups—and a primary reason why we are struggling to contain the threat.

A scientific approach to the phenomenon of terrorism is perhaps the purest way of viewing the topic. The very root of the word terrorism—"terror"—naturally provokes an emotional and personal response. Many Americans lost loved ones in acts of extreme violence perpetrated on 9/11 and the two major combat engagements fought in its aftermath. We also remember the horrific scenes broadcast live on the then-new CNN network of Marines being pulled out of the embassy rubble in Lebanon in 1983, and in 1985, we saw Navy diver Robert Stethem's lifeless body thrown from his aircraft onto the tarmac of the Beirut airport by Hezbollah hijackers. The bombing of the World Trade Center in 1993 and the Oklahoma City attack in 1995 again brought the horror of terrorism, foreign and domestic, into our homes, minds, and hearts.

There are many persistent disagreements regarding the rise of modern terrorism, such as those revolving around democracy, capitalism, and Christianity, all of which may make the United States a target… or hegemon and invader. The specific characterization of terrorism is also very difficult to define: criminal act, holy obligation, reaction to oppression, or freedom fighting? Each government agency has its own definition and interpretation, but we intuitively know, whatever the reason or definition, that one thing is crystal clear: terrorism is a threat to our national security. Investigating the terrorism phenomenon through a scientific lens eliminates both individual and institutional biases and removes emotions such as fear and anger. This approach also helps organizations move beyond sunk cost, "groupthink," and other unproductive and dangerous decision-making behaviors that have stymied our efforts to eliminate terrorist groups.

TERRORISM'S TARGET

Unlike many criminal activities, terrorist attacks are not indiscriminate, as we explore in later chapters through case studies and analysis. Targets are carefully chosen to assure the advancement of political or religiously motivated objectives. In soft targeting, the most vulnerable place will be selected as a way to maximize casualties—often venues where people will not be armed and will be paralyzed by the element of surprise. Perhaps it is helpful to think of terrorist targets in four categories: symbolic, functional, logistic, and expressive (Drake 1998).

Symbolic targets are attacked to elicit a psychological reaction, whether the assassination of a key political figure or the physical penetration or destruction of a government building or monument. Functional targets are obstacles to the success of the terrorist or group, such as the military, security officers, or opposing groups. Logistical targets are hit for financial profit, to obtain money or goods such as weapons, fuel, or

food. Kidnapping is a lucrative business for criminals and terrorists, and wealthy businessmen and their family members are logistical targets. Expressive targets are those hit as a response to emotion, for example, an attack on a lone American working for a nongovernmental agency in rural Africa. Expressive targets are not part of an overarching strategy and will not result in any political gain to the terrorist group. Usually, the victim was simply in the wrong place at the wrong time. Soft targets are a new addition to the playbook, complementing all of the preceding activities.

SOFT TARGET VIOLENCE: A COLLECTIVE TWENTY-FIRST CENTURY BLACK SWAN

The black swan theory is a metaphor describing a surprising event with major impact thought to be impossible, but then rationalized by observers in hindsight. The combination of low predictability and large impact of black swan events as related to nefarious groups and actors is central to this book's narrative concerning the asymmetric tactic of soft targeting.

In the first century AD, a Roman poet, Juvenal, called something presumed not to exist or deemed impossible a "black swan." Interestingly, Dutch explorer Willem de Vlamingh spotted a black swan in Australia in the 1600s while traveling through the area. The discovery of this creature, thought to be nonexistent, was deemed the "black swan problem" and introduced the concept of "falsifiability" to the scientific world. Scientists soon realized that that which they thought was unequivocally true might be proven otherwise. Modern black swan events were characterized by Nassim Nicholas Taleb in his 2010 book, *The Black Swan: The Impact of the Highly Improbable*. Taleb regards almost all exceptional scientific discoveries, historical events, and artistic accomplishments as black swans, or undirected and unpredicted occurrences. The rise of Adolph Hitler, the personal computer, the Internet, and the September 11 attacks are Taleb's examples of black swans. Taleb's comments in a *New York Times* article are important to frame our discussion regarding the social networking phenomenon:

> What we call here a Black Swan (and capitalize it) is an event with the following three attributes. First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable.
>
> I stop and summarize the triplet: rarity, extreme impact, and retrospective (though not prospective) predictability. A small number of Black Swans explains almost everything in our world, from the success

of ideas and religions, to the dynamics of historical events, to elements of our own personal lives.

Major axioms of the black swan theory include:

1. The disproportionate role of high-impact, hard-to-predict, and rare events beyond the realm of normal expectations in history, science, finance, and technology
2. The noncomputability of the probability of the consequential rare events using scientific methods (owing to the very nature of small probabilities)
3. The psychological biases making people individually and collectively blind to uncertainty and unaware of the massive role of the rare event in historical affairs

The theory refers only to unexpected events of large magnitude and consequence and their dominant role in history. Such events, considered extreme outliers, collectively play vastly larger roles than regular, predictable occurrences. In short, these are game changers, such as the rise of modern terrorist groups, cartels, and transnational organized crime groups. The advent of the domestic terrorist, a citizen who turns on his or her own government and kills innocent civilians to further his or her cause, might be considered a black swan.

Black swan logic makes *what you do not know* far more relevant than what you do know. Therefore, in the counterterrorism business, we should be exploring "antiknowledge" or what we do not know and what we do not expect from the enemy. In the security realm, we typically use specific data to make strategic decisions, instead of stepping back and viewing the entire issue with all of its complexities and changing environmental factors. We expect groups to engage in a similar manner as they have in the past, and we harden facilities and screen people accordingly. Unfortunately, we expend an inordinate amount of resources to prevent history from repeating itself, while the groups and individuals with a violent ideology work to hit us from an unexpected or asymmetric angle. As we discuss in Chapter 3, this resource drain and diversion of manpower is exactly what enemies hope to elicit, and we often play right into their hands.

The story of the Maginot Line shows how we are conditioned in this manner. After WWI, the French built a wall along the previous German invasion route to prevent reinvasion. However, Hitler simply went around the wall and marched into France. Over-reliance on past events as a predictor of future action, underestimating the creativity of the enemy, and the inability to think "outside the box" clearly leave us vulnerable. In black swan vernacular as related to terrorist events, history does not crawl, it jumps.

THE INTERNET AS A TOOL

Similarly, with the black swans of rapid technological and communication advances, we were wholly unprepared for how social networking would change our society, the definition of "community," and the manner in which people communicate. The Internet is a virtual world where people can be compelled (even unconsciously) to change their opinions, join movements, and even take up arms for a new, captivating cause. These new members are not forced to join; they are volunteers, who always make the best recruits in both licit and illicit groups. Sitting in their comfortable middle-class homes or at the local Wi-Fi–enabled coffee house, they do not have to be suffering, hungry, or uneducated to join in the dialogue. The impact of the Internet in the crime and terror realm was unforeseen and perhaps marginalized with the excitement of rapid growth, social networking sites, and virtual banking and commerce. Every piece of technology we enjoy—every application that makes our life easier or helps us communicate—is exploited by bad actors.

The main product of the terrorism marketing campaign is fear; however, by-products include recruitment, empathy seeking, and fundraising. As with all marketing operations, terrorism is meant to shift the public center of gravity through use of symbolism or themes, and these techniques can be overt or covert. We must also remember that, for many groups, this is a long crusade; the enemy is patient and thinks in terms of millennia, not years. Our children's children may indeed be struggling with the same terrorism and transnational crime issues with which we struggle today, and a quick fix is simply not possible.

Every day I scan numerous websites in an open source intelligence collection activity supporting research, lecture, and writing efforts. In the spirit of "know thy enemy," an axiom of the great war strategist Sun Tzu, I also access current web caches of various jihadi sites and the pages of domestic and ethnoseparatist terror groups. Often it is just the same day-to-day rhetoric; however, I have sensed a shift from outright violent threats to a more subtle, understated threat. For instance, Facebook pages appearing friendly and inviting will pull in the curious and then redirect them elsewhere for further discussion on edgier topics. Of course, many groups do not sugarcoat the message or their hate for the United States and also use the open forums to blatantly spread false information and propaganda. With the Internet, they are literally "hiding in plain sight" and, indeed, why should groups go underground when their Internet activities are perfectly legal? For a more in-depth examination of the exploitation of the Internet for recruiting, clandestine communication, and funding, please see my previous work on the terrorist–criminal nexus (Hesterman 2013).

The perpetrators of recent shooting events have even signaled their intentions in advance on social networking websites. On the night before he killed fifteen students and teachers at his former high school in Germany, Tim Kretschmer chatted on the Internet about his intention to commit mass murder. He wrote (Davies and Pidd 2009):

> I've had enough. Everybody's laughing at me. No one sees my potential. I'm serious. I have weapons and I will go to my former school in the morning and have a proper barbecue. Maybe I'll get away. Listen out. You will hear of me tomorrow. Remember the place's name: Winnenden.

Website administrators and users could become force multipliers if trained on what to look for, how to engage, and how, what, and where to report provocative comments such as Kretschmer's.

SOFT TARGETING MOTIVATIONS

We need to understand a group's or individual's motives to attack a soft target and what gains may be reaped from the event. The case studies in the book discuss specific operations; however, there are similar motivations and goals that cross all brands of terrorist and criminal groups:

- **Easier, cheaper, and short planning cycle.** Consider that the Kenya Westgate Mall attack planning cycle was just one year and executed with a small team of shooters with basic weaponry, whereas it took seven to eight years to plan the complex attacks of 9/11. The scope of the events differed, of course, with the events of 9/11 killing thousands and drawing the United States and its allies into protracted, expensive, and deadly wars in Afghanistan and Iraq. However, what if the target on 9/11 was the Pentagon City Mall in Arlington, Virginia, with 65 civilians killed and 175 wounded by al-Qaeda at the direction of Osama bin Laden? We likely would have followed the same military course of action into Afghanistan. Therefore, a smaller-scale soft target hit in the United States may carry the same weight as a large-scale operation to hit symbolic or hardened targets.
- **Increased likelihood of success.** The probability of a successful attack against an unprotected soft target is higher than against fortified hard targets.
- **Credibility.** A successful attack garners instant status for the group or cause.
- **Recruiting value.** Sympathizers are more likely to join the cause of a "winner."
- **Flexing muscle.** In the past five years, US government officials have repeatedly stated that al-Qaeda was drying up and

dying. Many thought the splintering was a sign of decline, yet the AQ 1.0 and 2.0 groups are successfully attacking and inspiring attacks. Government officials now say al-Qaeda is resurgent. Even small soft target attacks show the group is thriving and viable.

- **Compensating for weakness.** If a group does not have the resources to hit a hard target, or ongoing planning is moving too slowly, they can quickly hit a soft target.
- **As a last gasp.** If a group is declining, an easier soft target attack could be the last hope to recruit and gain credibility.
- **Backed into a corner.** When a group is trapped, the situation becomes extraordinarily dangerous. Consider the LTTE terrorist group case study in Chapter 8: when the group was corralled and boxed into one area of Sri Lanka, they took 100,000 civilians hostage on a beach and used them as human shields. This scenario is especially worrisome if dealing with a desperate religious group with apocalyptic intentions; its members may field their best weapon, possibly a WMD (weapon of mass destruction).
- **Test a new strategy, tactic, or weapon.** Hitting a soft target could be a dry run for a group that is honing an operation. It also could be used to assess emergency response and crowd evacuation procedures and to gather points for a later, larger attack that includes secondary or tertiary devices and possibly chemical, biological, or radiation agents.
- **Fund-raising.** Soft target attacks may result in kidnapping and hostage taking for ransom or in selling humans into slavery, such as was the case with the schoolgirls taken from their dormitory in Nigeria by Boko Haram. Piracy of a cruise ship or ferry could quickly raise tens of millions of dollars.
- **Quickly damage a market.** As witnessed with the airline industry after 9/11, the movie theater industry after the shootings in Aurora, Colorado, and attacks against resorts and hotel chains in Egypt, a soft target attack will immediately cause fear and avoidance of similar venues.
- **Delegitimize a government.** A successful soft target attack immediately casts doubt on the government's ability to protect its people, who will scrutinize intelligence operations, law enforcement, and first-response efforts. We already have a conspiracy theory-fueled public, with tens of thousands of "truthers" who not only distrust officials, but also believe events such as 9/11 and the Boston Marathon bombing were government "false flag" operations to cause fear and maintain tight control on citizens.
- **Cause political instability.** If properly timed, a soft target attack could change the course of an election and history. The group could get a candidate more favorable to its cause into office or repel voters from polling places. This type of political pressure

routinely happens in Mexico with the drug cartels, which violently engage prior to and during elections to shape outcomes by killing mayors, police chiefs, and political candidates.

- **Make a country look weak internationally.** A soft target attack such as the Boston Marathon bombing makes the country appear weak and unable to protect its citizens. Terrorists appear to be able to attack at will. A country that cannot protect its own people has difficulty convincing it can protect others.
- **To attain global media coverage.** A soft target attack will receive coverage in the 24/7 news cycle such as the live television coverage of the Beslan massacre, the Mumbai attacks, and the events of 9/11. If the group wants immortality, press coverage is the best course of action as the images of destruction and suffering are shown over and over. Many groups will broadcast on social media, even using Twitter during an event to air their grievances and inject more fear with threats of further attacks. Al-Shabaab terrorists were using Twitter throughout the attack on the Westgate Mall.
- **A target-rich environment.** Soft targets abound and groups can quickly bring a city to its knees, such as the Mumbai attack where a hospital, hotels, trains, and a train station were simultaneously targeted. In a small town, terrorists could hit a school, church, and mall all at once, or hit one and then the next in a campaign of terror. If the objective were to seize land and property, or even an entire small town, this type of timed multitarget operation may work in the United States as it has for the drug cartels in Mexico.
- **Psychological fear.** A successful soft target attack will wreak havoc on the psyche of the average citizen who may think, "Not only can my government not protect me, but even worse, it cannot protect my family." Perhaps nothing is worse than fear for the safety of your family, especially children. Specifically targeting women and children fuels the terror multiplier effect (TME).
- **Make a domestic issue international.** Hitting a soft target is a way to vault local or regional issues to the national scene, a hope of special-interest domestic terrorists such as those belonging to animal- and ecorights groups.

So, why hit soft targets? After considering the potential benefits, the answer is obvious: why not?

OUR UNIQUE VULNERABILITY

Perhaps the softest, most vulnerable target is you—the human being. Due to our culture and history, Americans tend to cast a psychological blind eye toward soft targets. In the aftermath of World War II, which

saw the mass slaughter of innocent civilians during combat operations by adversaries, the US government helped establish the 1949 Geneva Conventions, which protect noncombatants and civilians in and around the war zone (http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/). Therefore, our military doctrine is never to hit a soft target, even if the "most wanted" terrorist in the world is attending a religious service, visiting his child at school, or having a medical treatment. Instead, we will patiently wait for another opportunity to minimize collateral civilian casualties. We see the world through this lens, and believe (or hope) others will employ the same restraint.

Unfortunately, our enemies, foreign and domestic, do not play by the same rules. The new battlefields are in neighborhoods and communities, and civilians *are* the target. Terrorists have made this very clear in the United States with asymmetric attacks planned against civilian-rich, nonmilitary/nongovernment environments such as the Boston Marathon and Times Square. We routinely underestimate the sophistication of terrorists and criminals as they constantly exploit our vulnerabilities and naiveties to increase the chances of operational success. Also, for bad actors, there is no such thing as a "failed attack": every event is a learning experience. The free press typically overshares information about why the operation was successful or unsuccessful, and would-be attackers worldwide adjust their tactics. Professionals who fail to understand these emergent factors are at a disadvantage when protecting soft target venues, as we have transitioned to an entirely new security environment and paradigm in the last few years.

Hard targets including government buildings, military installations, and buildings with symbolic significance such as monuments have been further hardened over the years. Bad actors know hitting them not only will be more difficult, but also likely result in less shock factor to the American public. For instance, mass shootings on military installations such as the Navy Yard in Washington, DC, in 2013 and Fort Hood, Texas, in 2009 usually garner less public sympathy and outcry than those committed in schools, restaurants, and churches. Perhaps the occupants of these facilities are considered legitimate targets due to their occupation. This type of soft target rationalization pushes the would-be terrorist to strike elsewhere, to areas where the shock, outrage, and fear factors will be higher.

WHAT DO WE MOST FEAR?

Although typically avoided, we need to "go there" and desensitize when it comes to soft targets. What do we most fear? It seems the generations before us were much more adept at facing their collective fears and taking

steps to educate the populace, including children. The employment of the atom bomb in 1945 and the Soviet Union's attainment of nuclear capability in 1949 transformed the meaning of civil defense in the United States. During the early days of the Cold War, the government produced a video that taught children self-protection from a nuclear attack; the children practiced "duck and cover" exercises and were prepared to take care of themselves during attack if adults were not around (Mauer 1951). New York City issued 2.5 million identification bracelets, or dog tags, for students to wear at all times, with the unspoken purpose to help identify children who were lost or killed in a nuclear explosion. Over time and with the fall of Communism, the fear of nuclear attack waned along with civil defense exercises and preparation for WMD events. For decades, the government was quiet about threat and individual response.

After the attacks on 9/11, the Department of Homeland Security (DHS) attempted to re-engage in this realm and educate members of the public on how to protect themselves. For instance, on February 10, 2003, in response to intelligence information that terrorists were planning a WMD attack in the United States, DHS issued an advisory directing Americans to prepare for a biological, chemical, or radiological terrorist attack by assembling a disaster supply kit. Shelves were cleared of duct tape and plastic to seal homes and offices against nuclear, chemical, and biological contaminants. The DHS eventually faced ridicule and the advisory was jokingly referred to by comedians as "duct and cover." Certainly this type of response by the public should be factored into future advisories.

What types of trauma are experienced after an attack like those perpetrated on 9/11? Typically, there are changes of behavior; for instance, a community or nation may pull together during a mass casualty situation, putting differences aside for the greater good. However, an attack may cause ruptures in relationships and lead to suspicions and poor treatment, similarly to what Japanese Americans experienced during World War II after the Pearl Harbor attacks and the American Muslim community suffers today. In Kenya, following the Westgate Mall attacks by the Somali-driven al-Shabaab, Somali citizens were rounded up in the country and many deported. Also, after an attack, anniversary dates take on importance. For example, April, with anniversaries of the Columbine school attack (April 15), Oklahoma City bombing (April 19), and the Branch Davidian siege at Waco (April 20), is particularly tough for Americans and nervous security experts who fear copycats. Naturally, the September 11 date will always be burned into the national psyche, similarly to December 7.

When a domestic terrorist attacks fellow citizens, a sense of denial typically sets in and we search for some type of foreign influence to explain the behavior. This reaction could hinder the investigative

process, as it did immediately following the Oklahoma City bombing in 1995. The World Trade Center bombing executed by al-Qaeda had been just two years before, so the immediate assessment was the Murrah Federal Building had undergone a jihadist attack. I was working at the Pentagon at the time and vividly recall the discussions and assumptions being made by military planners. Naturally, they were influenced, as were all Americans, by the press, which fueled the fire with inflammatory baseless statements:

> "The betting here is on Middle East terrorists," stated CBS News's Jim Stewart just hours after the blast.
> "The fact that it was such a powerful bomb in Oklahoma City immediately drew investigators to consider deadly parallels that all have roots in the Middle East," piled on ABC's John McWethy.
> "Knowing that the car bomb indicates Middle Eastern terrorists at work, it's safe to assume that their goal is to promote free-floating fear and a measure of anarchy, thereby disrupting American life," the *New York Post* editorialized on April 20. "In due course, we'll learn which particular faction the terrorists identified with—Hamas? Hezbollah? the Islamic Jihad?—and whether or not the perpetrators leveled specific demands."
> "It has every single earmark of the Islamic car-bombers of the Middle East," wrote syndicated columnist Georgie Anne Geyer in the *Chicago Tribune* on April 21.
> Also on April 21, according to the *New York Times*'s A. M. Rosenthal, "Whatever we are doing to destroy Mideast terrorism, the chief terrorist threat against Americans, has not been working."

Even after the FBI released sketches of the suspects on April 24, the news media still would not let go of their assumptions. Thankfully, the VIN number from the vehicle used in the bombing was found at the scene and led to former soldier McVeigh, who was pulled over for speeding in a remarkable coincidence. Otherwise, the attack could have led us down the wrong path diplomatically and, possibly, militarily.

HOW SHOULD WE RESPOND?

A measured response to a terror event would be the best approach, although this is nearly impossible due to the proliferation of the Internet and 24/7 news broadcasts. As analysts and investigators, we need to avoid the "light pollution" that obscures the true threat as people gravitate and cluster around groundless theories as they did immediately

following the Murrah Building explosion. Fighting this clustering activity and being a skeptical empiricist is critical, as well as valuing and encouraging out-of-the-box thinkers who may identify and prevent a looming black swan event that hits the "reset" button in history. With regard to data analysis, any statistician will caution that we need to be careful of confirmation and distortion bias when looking at a terrorist attack situation. We also should not adopt a revisionist history of past attacks. Taleb calls this tendency the "triplet of opacity" and points out that how we understand history can be affected by three factors: the illusion of understanding, retrospective of distortion, and the overevaluation of facts.

Security fatigue is another phenomenon that is dangerous and exploitable. Americans are weary of long airport security lines and, now, a loss of communications privacy. Security is often inconvenient and especially trying for those unaccustomed to being targets. Therefore, we must find the right balance in our world and our places of work, education, worship, and play between living vigilantly and normally. In the end, however, personal security is a personal choice: If citizens choose not to face their fears and the threat and play out a potentially horrific scenario in their minds, they will likely respond poorly during a soft target attack.

After we prepare mentally to engage the soft target threat, understanding the motivations and emergent tactics of those who might strike is key to planning efforts. The next two chapters provide an introduction to international and domestic terror groups and the rise of soft targeting.

REFERENCES

BBC. "Malala: Shot for Going to School" (video) In *Panarama,* 2013.

Davies, Lizzy and Helen Pidd. "Germany School Killer Gave Warning in Chatroom," *The Guardian*, March 12, 2009.

DeHart, Jonathan. "Why Did the Taliban Shoot Malala?" July 18, 2013. http://thediplomat.com/2013/07/why-did-the-taliban-shoot-malala/

Dershowitz, Alan M. *Why Terrorism Works*. New Haven: Yale University Press, 2002.

Drake, C. J. M. *Terrorists' Target Selection*. New York: St. Martin's Press, 1998.

"The Geneva Conventions of 1949 and Their Additional Protocols." http://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/

Hesterman, Dr. Jennifer. *The Terrorist-Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups*. Boca Raton, FL: CRC Press, 2013.

Lewin, K. Defining the "Field at a Given Time." *Psychological Review*. 50: 292–310, 1943.

Mauer, Raymond J. "Duck and Cover—Bert the Turtle Civil Defense Film, 1951." http://www.youtube.com/watch?v=IKqXu-5jw60

Stern, Jessica. "The Protean Enemy." *Foreign Affairs* (Jul/Aug 2003).

Szilagyi, Marc J. and Andrew D. Wallace. *Organizational Behavior and Performance*. Glenview, IL: Scott, Foresman/Little, Brown Higher Education, 1990.

Taleb, Nassim N. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2010.

CHAPTER 3

International Terror Groups
Propensity and Ability to Mount Soft Target Attacks

> Russian soldiers are killing our children in Chechnya, so we are here to kill yours.
>
> **—Chechen fighter at the Beslan School massacre (Steele 2004)**

INTRODUCTION

After understanding the psychology of soft targeting and our vulnerabilities to the threat, it is important to comprehend the phenomena of postmodern terrorism: How did we arrive at this violent juncture in our history? And which actors have the propensity, reach, assets, and abilities to attack a soft target based on their past attempts or successful hits?

MODERN TERRORISM'S ROOTS

The era of modern terrorism began on July 22, 1968, with the hijacking of an airliner traveling from Rome to Tel Aviv by the Popular Front for the Liberation of Palestine, or the PFLP. The group, whose goal is the establishment of a Palestinian state, is still in business after 46 years. For five weeks, twenty-one passengers and eleven crew members were held hostage in Algiers as the world helplessly watched and learned about the PFLP cause. Eventually, the terrorists released the hostages, in exchange for sixteen Arab prisoners held in Israeli jails. This was not the first hijacking of an airliner; however, the PFLP's brazen use of the tactic to draw attention to its political cause, as well as concessions given by

Israel to the hijackers, ignited the phenomenon of modern terrorism as we know it today (Hoffman 2006).

The State Department has designated fifty-nine groups as foreign terrorist organizations (FTOs), which are actively engaged in some type of terrorist activity threatening our national security; this list has steadily grown throughout the last decade. A scan of the FTO list (Appendix A) illustrates the variety of worldwide terrorist threats, from dormant groups such as religious cult Aum Shinryko/Aleph in Japan, to the resurgent Irish Republican Army. Also included are separatist groups operating in only one country, such as ETA in Spain, to vast organizations such as al-Qaeda and its numerous affiliates around the world. Most, if not all, of the FTOs have targeted civilians to further their political or religious goals. Missing from the list, but providing an equally vexing and emergent national security threat are the fear-inducing global organized crime syndicates and Mexican cartel groups, which exhibit brutal tactics and are equipped like small armies.

Figure 3.1 depicts the successful rise of radical groups and modern terrorism. Early social and psychological science theorists had a

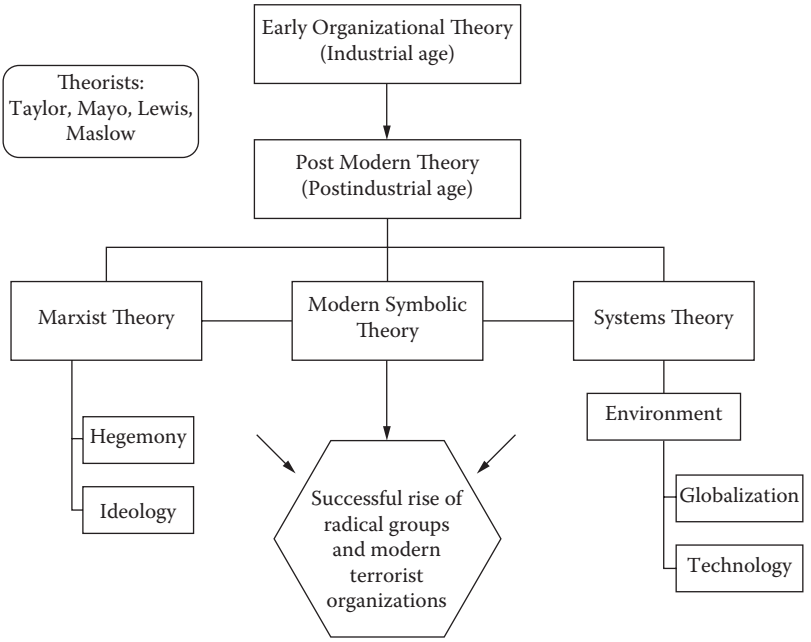


FIGURE 3.1 Organizational theories and the rise of modern terrorist organizations. (Hesterman, Jennifer. *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups*. Boca Raton, FL: CRC Press, 2013. With permission.)

substantial impact on the way we presently view and interact with organizations and their members. Postmodern theories and the associated thinking process build on this foundation and provide a remarkable means for understanding and diagnosing the emergence of revolutionary and terrorist organizations in the latter twentieth century. The discussion of the rise of postmodern terrorist groups is deeply rooted in the soft sciences; a fusion of psychology, sociology, and organizational development and behavioral theory allows insight into many of the vexing "whys" about the terrorism phenomenon. Understanding how our actions and the environment contributed to the rise of terrorism is key to better decision making with respect to response to terrorist threats and activity. For a detailed explanation of this original model, please refer to *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups,* Chapter 2, "Postmodern Terrorist Groups" (Hesterman 2013).

AQ AND AFFILIATES

> We remain at war with al-Qaeda.
>
> **—Matthew Olsen, director, National Counterterrorism Center (2012)**

Perhaps the most vexing and persistent threat to our national security is al-Qaeda (AQ), which has morphed from a centralized group to a high-performing, decentralized, leaderless organization. Although leader Osama bin Laden was killed in 2011 for inspiring and directing crimes against humanity, his death did not result in the dissolution of al-Qaeda; the radical ideology persists and serves as the glue holding this organization and its myriad affiliates together. After we destroyed much of their home base in Afghanistan, AQ has splintered and franchised, with global cells that train, equip, and fundraise independently. These cells also do not require the "permission" of a leader to carry out a mission; the battle cry has been issued, the original fatwas remain in force, and the target is the Western world and Islamic counries deemed too Westernized. An expert on modern terror networks, Marc Sageman (2003), calls this a "bunch of guys" hypothesis: members reinforce their group identities through the adherence to an ideological orientation and a strong bond of mutual commitment.

Like many emergent postmodern organizations, al-Qaeda and its offshoots are leaderless, yet high performing. In the book *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (Brafman and Beckstrom 2006), the authors assert the reason that al-Qaeda originally grew in power and persists is because bin Laden never assumed a traditional leadership role of the organization. The book uses

a very applicable illustration, discussing how the Apache Indians managed to hold off the Spanish army for over 200 years. They had no chief with positional power; they consistently chose and followed a *nant'an,* a spiritual and cultural leader who led by example and had no coercive power. The Apaches followed him because they *wanted* to, not because they had to. If a nant'an died, another would quickly step up and fill the void. Geronimo was a nant'an, and although he was never in an official leadership position, he had power and many wanted to take up arms and fight with him and on his behalf after his death. The Spanish army also failed to defeat the Apaches due to their loose organizational structure; power and operations were both decentralized. Raids on Spanish settlements could be planned, organized, and executed in three different places simultaneously. Attacks by the Spanish over time made the Apaches even stronger; they learned, adapted, and became even more dispersed and decentralized to frustrate their enemy. Interestingly, the operation to find and neutralize bin Laden was dubbed "Geronimo"—perhaps a nod to his mystique. The Apaches prevailed after the death of Geronimo, and al-Qaeda lives on after bin Laden.

The Ideology

Much has been written and discussed about the operational tactics of al-Qaeda. However, as the group morphs and persists, a lesser-studied and potentially more valuable topic is its glue and fuel: the radical ideology. We start with Sayyid Qutb, who was born in Egypt and moved to the United States to attend college in the late 1940s and early 1950s. His experiences as a college student in Colorado led to a hatred of the Western way of life; he believed the society was amoral and that women were promiscuous and too independent and outspoken. Upon graduation and return to Egypt, he joined the Muslim Brotherhood and quickly became a respected leader.

In 1952, Egypt's pro-Western government was overthrown by a group called the Free Officers Movement led by Gamal Abdel Nasser. Nasser initially appeared to court Qutb and the Brotherhood, although he was secretly plotting its demise. Once Qutb realized Nasser's intentions, he became an outspoken, forceful, and violent opponent of the ruling government, inciting the Muslim Brotherhood to action. The Nasser government cracked down on the dissidents, and Qutb was arrested in 1954, jailed, and routinely tortured. Eventually, he was left alone in prison and allowed some freedoms, including the ability to write. A prolific and powerful writer who masterfully used imagery and poetry to make his point, Qutb's two most important works were created during this period: *Fi Zilal al-Qur'an* (*In the Shade of the Qur'an*), and a

manifesto of his view of Islam, *Ma'alim fi-l-Tariq* (*Milestones*). Both of these works are still widely read and revered in the Islamist community and are recommended reading for all who want to understand the seeds of radicalism. The Egyptian government released Qutb from prison in 1964 by request of the Iraqi government; he immediately reconnected with the Muslim Brotherhood to plan the assassination of the Egyptian prime minister and overthrow of the ruling government. He was rearrested and executed in August 1966.

However, the damage was done: Qutb's timeless writings were his legacy, inspiring a school of thought called "Qutbism." Following Qutb's death, his brother, Muhammad, conducted lectures at King Abdulaziz University in Jeddah, Saudi Arabia—events regularly attended by Osama bin Laden. Qutb mentored Ayman al-Zawahiri, who went on to become a member of the Egyptian Islamic Jihad, mentor to bin Laden, and de facto leader of al-Qaeda after bin Laden's death. Qutb's writings inspired the latest generation of radical Islamists; while imprisoned in Yemen, Anwar al-Awlaki would read hundreds of pages a day of Qutb's works, stating that he was "so immersed with the author I would feel Sayyid was with me in my cell speaking to me directly" (Jones 2012). Later, al-Awlaki himself would inspire domestic terror attacks in the United States, such as the Fort Hood shooting and the actions of the Christmas Day "underwear bomber," Umar Farouk Abdulmutallab.

Rise of bin Laden and al-Qaeda

As a student of this subject, you have likely already studied the history of al-Qaeda. To grasp fully how bin Laden and his group emerged as arguably the most dangerous and successful terrorist group in history, I strongly recommend the award-winning books *Age of Sacred Terror* by Daniel Benjamin and Steven Simon (2002) and *The Looming Tower* by Lawrence Wright (2007). Both are extremely well written and should provide the basis for all academic discussions regarding al-Qaeda.

In the 1980s, inspired by his mentors, bin Laden left a lucrative engineering career and a young family to volunteer in Afghanistan and assist the mujahedin-led and US-supported fight against the Soviet Union's infiltration of what was considered holy and sacred Muslim land. As the Soviets withdrew in the late 1980s, Abdullah al Azzam, the architect of the successful war and his protégé, bin Laden, were left with a network of at least 10,000 Islamists. Azzam and bin Laden formulated a plan to use these forces to form a new group called *al-Qaeda,* meaning "the base," and take their cause to other countries, not specifically to the West. However, any goodwill toward the West for its help in Afghanistan evaporated in 1990 when the United States postured

for Operation Desert Storm, in support of Iraqi-invaded Kuwait. Bin Laden, who returned to Saudi Arabia in early 1990 as a hero for his efforts in Afghanistan, met with King Fayd and pleaded with him not to accept Western help with repelling Iraq from Kuwait and protecting the kingdom. He was rebuffed and went underground, plotting his revenge against the West while military operations were underway in the region. His first attack was the simultaneous bombing of two hotels in Aden, Yemen, on December 29, 1992, where US troops were thought to be residing. A few months later, on February 26, 1993, the first attack on the World Trade Center was executed by Ramzi Yousef, nephew of Khalid Sheikh Mohammed (KSM), who was at the helm of operational planning. Yousef and KSM then planned the 1994 "Bojinka" plot to destroy US-flagged airliners in the Pacific, but their plan unraveled when a practice bombing by Yousef failed to bring down the plane and a subsequent investigation uncovered the plot. The 1998 simultaneous embassy bombings in Africa and the 2000 bombing of the *USS Cole* further raised al-Qaeda's profile and strength. But the catastrophic attacks on 9/11 would be bin Laden's greatest accomplishment, just nine years after his first attack against the West.

Emergent al-Qaeda

Al-Qaeda made its initial appearance on the State Department's foreign terrorist organization (FTO) list in 1999, in light of the embassy bombings the previous year. In 1999, the FTO list consisted of only twenty-eight groups; the 2014 list contained fifty-eight groups, with over half being radical Islamist al-Qaeda offshoots or affiliates (Appendix A). Twenty-six organizations on the original 1999 list remain, a testament to the staying power of modern terrorist organizations.

AQAP

After the 9/11 attacks and our subsequent military operations to destroy its base in Afghanistan, al-Qaeda scattered to safe havens in the Middle East, including Yemen, the ancestral homeland of the bin Laden family. Al-Qaeda in the Arabian Peninsula (AQAP) quickly formed and grew in strength. The group was founded by Said Ali Al Shihri and Ibrahim Suleiman Al Rubaysh, both former Guantanamo Bay detainees whom the United States released to the Saudi deradicalization program. Unfortunately, both these terrorists left the Saudi program, made their way to Yemen, and joined two other terrorists, Nasir Al Wuhayshi and Qassim Al Raimi, who had escaped from Yemeni prisons. Together, these four terrorists built AQAP into a formidable transnational enterprise. Al

Shihri was killed by a drone attack in Yemen on September 10, 2012. Al Wuhayshi, who is AQAP's leader, was seen in a video on April 16, 2014, addressing a large group of AQAP fighters in public in Yemen, threatening to eliminate the United States. Despite a series of airstrikes following the AQAP meeting, Saudi citizen Ibrahim al-Asiri—an expert bomb-maker for AQAP and the mastermind of several attempts against the United States, such as the failed bombing of an airliner over Detroit on Christmas Day 2009—remains at large.

AQAP attracted supporters such as Anwar al-Awlaki, a US citizen and radical Islamist. Al-Awlaki was born in the United States and obtained a BS degree (civil engineering) from Colorado State University, an MA (education leadership) from San Diego State University, and worked toward a PhD at George Washington University. Inspired by the writing of Qutb, al-Awlaki met with and encouraged the 9/11 hijackers at the Dar al-Hijrah mosque in northern Virginia and persuaded and supported Nidal Hassan's plan to kill soldiers at Fort Hood through eighteen e-mails sent from abroad. He met Christmas Day airline terrorist Umar Farouk Abdulmutallab at an al-Qaeda training camp in Yemen and inspired and encouraged Faisal Shahzad to bomb Times Square. In a somewhat controversial move, the US government targeted and killed al-Awlaki in a drone attack in Yemen in 2011. Also killed in the vehicle was the editor of *Inspire,* al-Qaeda's online magazine used for recruitment and rhetoric, and to educate followers on bomb-building and terrorist tactics. The killing of al-Awlaki rekindled a long-standing debate about the definition of a "terrorist" since he was not a trigger puller, but rather the inspiration behind attacks. The United States was sending a clear and unequivocal message: If you provide logistical support or, in this case, the ideological fuel fanning the flames of radicalism, you are a terrorist and a legitimate target.

By utilizing Internet archive services, it is possible to read al-Awlaki's writings and interaction with his followers (http://wayback.archive.org/web/20110707150524*/http://www.anwar-alawlaki.com/). Through his words, we can better understand his psychological and sociological construction, how he radicalized, and his initially quiet ascendance to power as a spiritual leader of a religious terrorist group. The comments of hundreds of followers posted on his blog give great insight to hatred against the West, and there are repeated calls by all for the destruction of the United States.

Other AQ Splinter Groups

In the years following the 9/11 attack, al-Qaeda affiliates grew worldwide in at least fifteen countries. These "al-Qaeda 1.0" groups have also now splintered into "al-Qaeda 2.0" groups:

- *Al-Qaeda in Iraq (AQI), now known as the Islamic State of Iraq and the Levant (ISIL or ISIS):* Operations in Iraq led to the rise of Islamic state of Iraq, or AQI, which has been responsible for horrific attacks against coalition forces, mosques, and the country's new leadership following the ouster and death of Sadaam Hussein. The original goal of AQI was to force the withdrawal of coalition forces from Iraq. The troop pullout in 2013 emboldened efforts to establish a foothold in the country and infiltrate the newly established government. Lured by Syria's civil war, AQI fighters entered the northern part of the country and began recruiting members, possibly up to 2,000, and it challenged the Jabat al Nusra al-Qaeda splinter group for control. In 2014, AQI began hitting targets inside Lebanon and Turkey, pushing violence across the Syrian border and into neighboring countries. In January 2014, ISIS seized Fallujah from the Iraqi government, declaring it an Islamic state and its home base. The recapturing of Fallujah by the insurgents was a major victory against coalition forces that had fought long and hard for control of the city. ISIS is slowly encroaching on Baghdad, and security experts fear the group will ultimately attempt to overthrow the government. In May 2014, an ISIS-trained Frenchman who had traveled to Syria last year to join with radical Islamist fighters there, Mehdi Nemmouche, killed three tourists at the Jewish Museum in Brussels. He escaped from the scene but was caught during a routine customs check on Friday as he arrived by bus in Marseille from Brussels. He was carrying an assault rifle and revolver used in the shooting. He was the first European trained by an al-Qaeda affiliate to carry out an attack in Europe. By September 2014, ISIS commandeered a wide swath of Syria and Iraq, claiming a caliphate. The group's plan to spread throughout the Middle East, as well as into Europe, India, and Indonesia was revealed on USBs and computers seized during military operations in Syria and Iraq. The group also planned WMD attacks, including Y pestis, or bubonic plague. ISIS has specifically threatened the United States, posting pictures of their operatives standing in front of key targets such as the White House, a mall in Charlotte, North Carolina and landmarks in Chicago. The terrorist group released a specific message for Americans via Twitter, stating "We are in your state; we are in your cities; we are in your streets."
- *Al-Nusra Front for the Protection of the People of the Levant (Jabhat al-Nusram):* Jabhat al-Nusram is a jihadist al-Qaeda

affiliate emerging from the civil war in Syria. The group was possibly fed by Muslim Brotherhood members who simply walked into Syria from Egypt during the chaotic 2011 Arabic Spring uprisings in the region when key border crossings were left unguarded. Within months of formation, the group orchestrated a simultaneous car bombing of the main intelligence complex in Damascus, using 1,000 kilograms of explosives and killing at least fifty-five people and injuring four hundred others. Leveraging the Internet, the group communicates regularly with the populace to organize riots within the country. In April 2014, the group opened a new front in the war, attempting to seize control of oil fields in the eastern part of Syria. The Al-Nusra Front is battling ISIS in Syria, the first example of two AQ splinters fighting for territory.

- *Tehrik-e-Taliban Pakistan (TTP):* TTP is a loose alliance of militant groups in Pakistan, affiliated with the Afghani Taliban and the force behind the failed Times Square bombing attempt. TTP provided training and logistics to American Faisal Shahzad, subsequently landing on the State Department's FTO list within days of the event. The group has also moved into Syria to assist the rebel factions.
- *Harakat al-Shabaab Mujahideen (al-Shabaab):* Al-Shabaab (meaning "the youth") operations in Somalia exploited the country's continued descent into lawlessness, possibly exacting proceeds from pirating operations in the Gulf to fuel its growth. An American commander in al-Shabaab, Abu Mansur al-Amriki, grew up in Alabama as Omar Shafik Hammami; he radicalized and fled to Somalia in 2006 to join the effort, quickly rising through the ranks to become its leader. Al-Amriki was surprisingly killed by al-Shabaab in 2013, after a falling-out with the group over videos he posted on YouTube that were deemed to be narcissistic. Amriki's hypnotic, rap-styled music was used to entice Americans to join al-Shabaab in Somalia. His "First Stop Addis" has disappeared and reappeared many times on YouTube, but a simple keyword search will pull up the latest version. The music is almost mesmerizing and the message clear and compelling; Amriki himself sings the lyrics. As we continue to study how the radicalizing switch gets turned from "off" to "on" in the human brain, these videos provide insight into how the enemy is tapping into certain messages and themes to persuade, encode, and then distribute through the Internet. Clearly, the use of rap in this video is a marketing tool to target demographically. One of al-Shabaab's most fertile recruiting grounds is Minnesota, home

to the largest Somali population in the United States. Shirwa Ahmed and Farah Mohamad Beledi, the first two confirmed US suicide bombers, traveled from Minneapolis to Somalia to receive al-Shabaab training. Other Somali American recruits have come from Ohio, California, Virginia, New Jersey, and New York, according to a list compiled by the Anti-Defamation League (Council on Foreign Relations 2013). In 2012, US Army veteran and intelligence specialist Craig Baxam was arrested in Kenya, boarding a bus to Somalia with the intent to join al-Shabaab. Several recruits successfully traveled to Somalia and died in suicide bombings; others were arrested in the United States as they prepared to leave the country. It is estimated that over forty Americans have gone to Somalia to fight for al-Shabaab, a trend the FBI has describes as a top domestic terrorist threat (CNN 2013). The concern is that they will return home with tactics and training that can be used inside the United States. Al-Shabaab controls the southern part of Somalia and has started recruiting heavily from neighboring Kenya, which engaged through the 2011 Operation Linda Nchi, targeting al-Shabaab's training camps with aerial bombing campaigns. Although it declared its loyalty to al-Qaeda in 2008, this relationship was formally cemented in 2012 with a proclamation from Ayman al-Zawahiri welcoming the group and its members to al-Qaeda. Following the announcement of formal ties with al-Qaeda, at least 500 al-Shabaab fighters traveled to Yemen in 2012 to join AQAP. Al-Shabaab was responsible for the expertly planned and executed operation against the Westgate Mall in Nairobi in September 2013, killing sixty-seven people and injuring 175; this attack is covered in depth in Chapter 5.

- *Al-Qa'ida in the Islamic Maghreb (AQIM):* AQIM is centered in Algeria, where it has launched an insurgent campaign to turn the country into an Islamist state. AQIM arose from Salafist Group for Preaching and Combat, GSPC, and the group mainly engages in hostage-taking and ambushes against government leaders and law enforcement. After standing up the Boko Haram group in Nigeria in 2009, the AQIM was quiet until the kidnapping of several European tourists from the Timbuktu, Mali, UNESCO World Heritage site in 2011 and their execution in 2013. Also, AQIM took responsibility for a September 2013 car bombing in Timbuktu that killed two civilians. A major battle at Timbuktu that saw the destruction of ancient buildings and artifacts was likely initiated and fueled by AQIM. In 2013, an AQIM splinter faction seized control of an oil field

in Algeria to protest France's involvement in neighboring Mali. Using helicopters and assault weapons, the terrorists took over the facility, randomly killing workers and taking six hostages, including Americans. Unfortunately, all were killed in a botched rescue attempt by the Algerian government.

- *Boko Haram (AQIM splinter):* Boko Haram, meaning "Western education is sin" in the local Hausa language, is a jihadist militia with ties to AQIM that has attacked churches and government buildings in an attempt to establish Sharia law. The group has carried out hundreds of brutal attacks in Nigeria since its formation in 2011, killing thousands. In the period from January to March 2014, Boko Haram was responsible for the brutal killings of almost 1,800 civilians. Strict Islamists, members of Boko Haram have been responsible for horrific soft target attacks against Christians in Nigeria, with many fleeing the country in fear after their villages and churches were razed and burned to the ground. In 2014, the group escalated its campaign against churches, striking at least one per week. Boko Haram has singled out women and girls in its campaign of fear; the group was responsible for the kidnapping of 275 girls from a boarding school in April 2014. The group's leader, Abubakar Shekau, stated: "There is a market for selling humans. Allah says I should sell. He commands me to sell. I will sell women. I sell women" (Shekau and Levs 2014). However, not all Nigerians are against the presence of Boko Haram, with one stating: "If I was attacked by Boko Haram, it's like being attacked by God. It's God's wish and I have no problem with that" (Raghavan 2012). The Nigerian military has been unable to engage or disarm Boko Haram, and the country seems to be resolving itself to its brand of ruthless violence. Instability in Nigeria is also being exploited by Iran, which is creating a "Nigerian Hezbollah," known as Islamic Movement of Nigeria (IMN). The group's leader, Sheikh Ibrahim Zakzaky, draws inspiration from Hezbollah leader Nasrallah, whose picture is carried at IMN demonstrations.
- *Chechen separatists:* The Islamist Chechen separatists fighting Russia have ties to al-Qaeda dating back to 1999, when their leaders visited bin Laden in Khandahar, Afghanistan. Following the hostage-taking at Moscow's Dubrovka Theater in 2003, the State Department designated three Chechen groups as terror organizations: the Islamic International Brigade, the Special Purpose Islamic Regiment, and the Riyadus-Salikhin Reconnaissance and Sabotage Battalion of Chechen Martyrs.

> Chechen terrorists prefer to hit soft targets such as theaters, schools (Beslan attack of 2004), train stations, and trains. The Chechen "black widows" are ruthless female terrorists who typically carry out suicide bombings against targets; the original group consisted of vengeance-seeking women widowed by Chechen operations. The Boston Marathon bombers, the Tsarnaev brothers, were of Chechen descent and were at the very least influenced by Chechen radical Islamist ideology.

Although the al-Qaeda affiliates may struggle in the face of stepped-up US and regional engagement, they remain a formidable and flexible force, moving to and operating in areas of conflict and lawlessness, preying on the vulnerable populace.

Bin Laden Speaks

On May 2, 2011, a US-led military team entered a compound in Abbottabad, Pakistan, and killed Osama bin Laden. A trove of sensitive site exploitation (SSE) material was removed from the compound for analysis, with seventeen documents released to the public. The 2012 study "Letters from Abbottabad" (Combating Terrorism Center, West Point) analyzes the seventeen declassified documents gathered during the SSE operation at the compound, providing outstanding insight and analysis of bin Laden's unyielding role in shaping al-Qaeda and the affiliates, as well as activities assisting other terrorist groups (US Military Academy 2012). Bin Laden opined about conducting a mass attack on communications systems, targeting railroad infrastructure, and striking smaller US cities. He also pondered ways to use the media in his favor and to induce political dissent in our system. Despite being in exile from the group, the documents revealed that he had a hand in nearly all of the major terrorist attacks since 9/11, including the siege in Mumbai.

AQ's New Goals and Tactics

According to terrorism expert Bruce Hoffman (2010), al-Qaeda's goals are changing and this impacts how they target us. His key points include:

1. Al-Qaeda is increasingly focused on overwhelming, distracting, exhausting us.
2. In the wake of the global financial crisis, al-Qaeda has stepped up a strategy of economic warfare.
3. Al-Qaeda is still trying to create divisions in alliances by targeting our partners.

4. Al-Qaeda is aggressively seeking out, destabilizing, and exploiting failed states and other areas of lawlessness.
5. Al-Qaeda is actively seeking recruits from non-Muslim countries who can be easily deployed for attacks in the West.

Often called the "death by a thousand cuts" strategy, AQ's strategy is to exhaust and overwhelm our government and people. The FBI (2012) often reminds us that, in a 2004 video, bin Laden stated he "bled Russia for 10 years until it went bankrupt and was forced to withdraw in defeat … We are continuing in the same policy to make America bleed profusely to the point of bankruptcy." Of course, the low cost to execute the 9/11 attacks and the resulting devastation to our economy from extensive military engagement overseas have not gone unnoticed by groups wishing to do us harm. Dragging us into a "long slog" is not just a hope, but an operational tactic.

HEZBOLLAH

> American terrorism is the source of every terrorism in the world.
>
> **—Hassan Nasrallah, Hezbollah leader**

We must remember that, prior to 9/11, Hezbollah was responsible for the deaths of more Americans than any other terrorist group. The group had a hand in the 1983 bombing of the Marine barracks in Beirut (241 US military dead, sixty wounded), the kidnapping and murder of US officials in Lebanon, and the 1996 Khobar Towers bombing in Saudi Arabia (nineteen US military dead, 372 wounded). When tensions escalate between the United States and Iran or Syria, Hezbollah inevitably starts a campaign of saber rattling and threats of strikes against our country. Perhaps no group is better positioned to strike within the United States, as Hezbollah has a strong presence north and south of our border, as well as internally with fund-raising cells and sympathizers. The potential for an undetected sleeper cell to lash out upon direction from one of its sponsors, Iran or Syria, cannot be overlooked.

Hezbollah has been in operation for 33 years and was designated as an FTO by the State Department in 1995. The group is complex in nature with several "arms," including military, political, and community support. This complexity makes engagement extremely difficult. For example, due to the comingling of activities, sanctioning one of its "charities" often means taking money away from the needy as well as militants. The group is now global, with a presence in Central and South America, Western Africa, and Europe, operating in the same "space" as other major terror groups such as the Revolutionary Armed Forces of

Colombia (FARC) and al-Qaeda. The liaison of Hezbollah with these groups, sharing tactics, trafficking routes, etc., is of great concern. The group vigorously raises funds in the United States through charities and intellectual property crime, especially through selling knock-off designer purses, DVDs, baby formula, and high-demand pharmaceuticals such as Viagra (Hesterman 2013).

Despite decades of overt and covert attempts to dismantle the group, it is still one of the world's most effective terrorist organizations. A review of Hezbollah reveals an organization that leverages unique sources of power and continues to wield influence in the Middle East as well as globally.

Methodology and Objectives

Hezbollah has a history of suicide bombing attacks; however, this tactic appears to have fallen out of favor in the past ten years. Kidnapping has been very effectively utilized as a way to engage in prisoner exchange and Hezbollah also fields a unique weapon: the group is very adept at leveraging the world audience through press campaigns, political activity, and humanitarian engagement.

Primary Area of Operations

Hezbollah operates in the formerly Syrian-controlled Bekaa Valley, the southern suburbs of Beirut, and southern Lebanon. The State Department's "Country Reports on Terrorism" gives a glimpse into its global reach, stating that Hezbollah has established cells in Europe, Africa, South America, North America, and Asia. The group's training bases are mostly in the Bekaa Valley, with headquarters and offices in southern Beirut. Hezbollah is now a "state within a state," similar to how the Palestinian Liberation Organization used to operate in Lebanon.

Tactical Proficiency

According to the US State Department (2010) and the FBI, Hezbollah is the most technically capable terrorist group in the world.

Active and Deadly

The following is a timeline of major Hezbollah activity in the last eight years.

2014: Hezbollah is heavily engaged in the Syrian conflict, working with the Assad loyalist militia known as al-Jaysh al-Sha'bi, which was created and is maintained by Hezbollah and Iran's Islamic Revolutionary Guard Corps-Qods Force. Hezbollah has pushed Syrian conflict violence across the border into Lebanon and Turkey.

2012: On July 18, Hezbollah attacked Israeli tourists boarding a bus at Bulgaria's Burgas airport. Five Israeli citizens, a Bulgarian bus driver, and the bomber were killed. A similar attack was planned in Cyprus.

2011: Hezbollah was reportedly behind a bombing in Istanbul in May 2011, wounding eight Turkish civilians in a possible assassination attempt on the Israeli consul to Turkey.

2009: When Israel engaged Hamas in Gaza, Hezbollah did not intervene militarily (possibly at the behest of Syria), but influenced the battlefield in a variety of ways. Prior to the conflict, Hezbollah's leadership invited Arab nations to join it in protesting Israel's embargo of goods entering Gaza. Their tactic contributed to the propaganda associated with the conflict and also demonstrated Hezbollah's ability to engage from afar via psychological operations.

2008: After three days of bloodshed, heavily armed Hezbollah fighters seized West Beirut. This was the first use of Hezbollah's military arsenal against its host nation to increase territory and span of control. The conflict was sparked when the government attempted to shut down Hezbollah's vast telecommunications network.

2006: Hezbollah militants kidnapped two Israeli soldiers in northern Israel, sparking the month-long "Lebanon war," which devastated the country's infrastructure. During the conflict, Israel bombed Lebanon and deployed troops and tanks and Hezbollah fired 4,000 rockets across the border into Israel. In all, more than 1,000 Lebanese (mostly civilians) were killed, and 120 Israeli soldiers and forty-three Israeli civilians lost their lives.

Operations in the Western Hemisphere

Hezbollah continues to expand its sphere of influence methodically around the world while receiving weapons and training support from Iran and Syria.

South America

Hezbollah's activity in the Western Hemisphere is of great concern. For instance, the group has a stronghold in South America, especially in the triborder area, where Paraguay, Brazil, and Argentina intersect.

Approximately 25,000 immigrants from Lebanon came to the area in two waves: after the 1948 Arab/Israeli war and, in 1985, after the civil war in Lebanon. Hezbollah has garnered support from these communities and is heavily engaged in charitable fund-raising, DVD piracy, tax evasion, and money-laundering schemes, as well as other money-making ventures. In 1992, Islamists attacked the Israeli embassy in Buenos Aires, Argentina, with a car bomb, killing twenty-nine people and injuring more than 250 others. The Islamic Jihad organization, directly linked to Hezbollah, claimed responsibility. In 1994, Hezbollah used a truck bomb to attack a Jewish community center in Buenos Aires, killing eighty-seven people and injuring hundreds. Investigators linked the plot directly back to Iran, which also executed copycat bombings, just eight days later, attacking the Israeli embassy and a Jewish community center in London.

The triborder region is not the only Hezbollah stronghold in the region. In 2009, the SOUTHCOM commander testified that a Hezbollah presence was detected in Colombia, and the group is heavily involved in the drug trade (Senate Armed Services Committee 2009). A final concern is that Hezbollah's liaison with al-Qaeda in Latin America was documented as far back as November of 2002. At that time, intelligence agencies reported a "summit" meeting took place in Ciudad del Este between Hezbollah leaders and other radical Islamist terrorist groups, including al-Qaeda (Boettcher 2002).

Venezuela's long-term, established liaison with Hezbollah is also worrisome. In 2006, following the end of hostilities in Lebanon with Israel, Hezbollah's leader, Hassan Nasrallah, called the now deceased Hugo Chavez his "brother," and signs reading "Gracias, Chavez" were hung to thank him publicly for his support. In response to the Israeli engagement in Gaza in 2009, President Chavez ejected the Israeli ambassador and staff from his country. Chavez openly invited Hezbollah members to live in Venezuela, and his embassies in the Middle East have been used to launder Hezbollah money, according to investigation by the United States. Chavez's replacement, President Nicolas Maduro, continues to court Hezbollah and asked for the group's assistance during student uprisings in 2014. State Department-sanctioned Hezbollah terrorist Ghazi Atef Nassereddine is now living in Venezuela and gives updates in Spanish via his Twitter account (@GhaziAtef).

Canada

Undeniably, Hezbollah has a very strong presence in Canada. In 2012, the United States uncovered a Hezbollah-related scheme to launder the proceeds of narcotic trafficking and other crimes through Lebanese financial institutions, with amounts totaling over $480 million. Proceeds were moved through West Africa, and the buying and selling of used

cars was employed as a method of moving the dirty money. One bank of interest connected to the laundering was a Lebanese-Canadian institution, which forfeited $150 million of proceeds from the scheme. In a preview chapter from his upcoming book, *Hezbollah: The Global Footprint of Lebanon's Party of God,* terrorism expert Matthew Levitt (2012) reveals Hezbollah activated suspected "sleeper cells" in Canada to carry out an attack to avenge the targeted killing of Imad Mughniyeh.

An interesting case of a possible Hezbollah sympathizer was that of Khaled Nawaya, who was born in Saudi Arabia, but is of Syrian descent. He moved to the United States at the age of seventeen and earned two degrees, in aeronautics and management. He was a flight instructor, but lost his student visa status in the United States, filing and winning a lawsuit against Embry Riddle University for providing "bad immigration advice." He requested and was approved for residency in Canada. On October 6, 2009, Nawaya lied to the Border Patrol when trying to cross into British Columbia during his move north. When repeatedly questioned about the amount of currency in his vehicle, he adamantly stated he had less than the $10,000 required by law to be declared. However, Nawaya actually had $800,000 in gold coins, another $70,000 in cash in the vehicle, and $10,000 in cash on his person. Contents of the vehicle included a ring bearing the insignia of the terrorist group Hezbollah, 9/11 conspiracy theory-themed DVDs, and a scarf adorned with the images of a former Israeli prime minister and a US president depicted as monkeys (Armstrong and Freeze 2009).

Prior to his trip, Mr. Nawaya wired US$1 million to his brother overseas, who bought the Canadian gold coins on the Internet and had them shipped to Mr. Nawaya in the United States. Mr. Nawaya then loaded the coins into his car in the United States and attempted to drive them across the Canadian border. Canadian authorities labeled the case a "probable national-security nexus" and detained Mr. Nawaya for one month, eventually releasing him due to inability to establish a case. However, he was charged with his failed declaration under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, and his money was confiscated. We may never know his full intentions and whether he was a Hezbollah sympathizer, but the case is worthy of consideration. In 2011, he petitioned to have his US visa reinstated, but his request was declined.

At the Mexican Border

The number of Hezbollah operatives operating in Mexico has increased in recent years. In 2009, former Syrian military officer Jamal Yousef was arrested in New York City on narcoterror charges for his involvement in a weapons-for-cocaine scheme between Hezbollah and FARC, using Mexico as a safe haven. According to the indictment, a weapons cache

of 200 rifles, 2,500 hand grenades, C4 explosives, and antitank munitions was stolen from Iraq by Yousef's cousin, a member of Hezbollah, and moved to the home of family members in Mexico, also affiliated with the terrorist group. Yousef planned to deliver the weapons to FARC in Colombia, in return for 2,000 pounds of cocaine, but the Drug Enforcement Agency (DEA) intervened. Yousef pled guilty and was sentenced to twelve years in prison (US District Court, Southern District of New York 2009).

Although he is widely believed to have been a lone operator, Jameel Nasr was an international Hezbollah operative, taking direction from Lebanon to establish a Hezbollah network in Mexico and throughout South America. Nasr traveled regularly between Lebanon, Venezuela, and Tijuana, Mexico, and was arrested in 2010 by Mexican authorities upon his return from one of these trips. Mexican authorities said that Nasr had been "entrusted with forming a base in South America and the United States to carry out operations against Israeli and Western targets" (Investigative Project on Terrorism 2010).

In late 2011, prosecutors in Virginia charged a Lebanese man, Ayman Joumaa, with smuggling at least "tens of thousands of kilos" of Colombian cocaine into the United States, with 85,000 kilos sold to the Los Zetas cartel. Joumaa and his associates laundered over $250 million in proceeds through Spain, West Africa, Lebanon, Venezuela, and Colombia (US District Court for the Eastern District of Virginia 2009). According to the US Treasury Department, Hezbollah derived financial support from the criminal activities of Joumaa's network through the sanctioned Lebanese Canadian National Bank of Beirut (Rotella 2011). In 2011, a former undercover law enforcement officer discussed the Hezbollah interface with drug trafficking organizations (DTOs), saying the group receives cartel cash and protection in exchange for giving its expertise on subjects ranging from "money laundering to firearms training and explosives training." He also discussed his discovery of Hezbollah safe houses in Tijuana and Durango (KGTV News, San Diego 2011).

Tunnels Hezbollah has constructed a network of tunnels in Lebanon that are used to secure the group from Israeli airstrikes and permit covert maneuvering of forces. The tunnels have medical facilities, dormitories, lighting, heating and cooling systems, and even digitally controlled surveillance and weapon systems. Recent reports from Beirut indicate that with the help of Iran, Hezbollah has tunneled mountains in the Bekaa region and into Syria (Yaghi 2012). Hamas has also constructed a network of 400 main and 1,000 feeder tunnels between the Gaza Strip and Egypt, many of which can accommodate vehicles. Their tunnels are used to smuggle weapons, personnel, medicine, construction material, fuel,

and other goods embargoed due to the ongoing Israel–Palestine conflict (Zaboun 2012).

Tunnels built by Mexican drug trafficking organizations to cross clandestinely from Mexico into the United States have grown increasingly sophisticated. Law enforcement agents have discovered more than 150 tunnels since 1990, most crude and incomplete, but a few operational with tracks to move carts loaded with contraband across the border. In July 2012, DEA and Immigration and Customs Enforcement (ICE) agents discovered, under a strip mall in San Luis, Arizona, a 240-yard, $1.5 million tunnel that was expertly constructed, with 6-foot ceilings and wood walls and equipped with ventilation, lighting, hydraulic systems, and other high-tech components. This was not the common dirt tunnel through a sewer system previously found. DEA agents believed the tunnel was the work of experienced engineers (Spagat and Billeaud 2012). If Mexican cartels want better tunnels, they will recruit the expertise they require. A former US law enforcement agent with extensive experience working undercover in Mexico believes the expertise and construction features seen in the latest cartel tunneling efforts point to Hezbollah's involvement (KGTV News, San Diego, April 18, 2013).

Bombs A new weapon in the cartel's battle for control seems to have been imported directly from Middle Eastern terror groups and debuted in July 2010 with the successful detonation of a vehicle-borne improvised explosive device (VBIED) in the border city of Ciudad Juárez. The Juárez cartel deliberately targeted first responders by placing a bound, wounded man in a police uniform at the scene, luring law enforcement and medical personnel to the area. A nearby vehicle, inconspicuously laden with 22 pounds of Tovex, exploded moments later, killing three people and wounding twenty. Tovex is a water gel explosive widely used as a substitute for dynamite for industrial and mining purposes. Theft of Tovex in Mexico is a common occurrence; in February 2009, masked gunmen stole 900 cartridges of the substance from a US firm in Durango, Mexico (Caldwell 2010).

In July and August 2012, a wave of car bombings in northeast Mexico targeting a city hall and the homes of security officials were detonated by Zeta and Gulf cartels as part of their campaign to influence local elections. Two of the bombs were sophisticated and detonated by use of a cell phone. VBIEDs are widely used by insurgents in Iraq and Afghanistan and terrorist groups such as Hezbollah and al-Qaeda. Richard Schwein, the former FBI special agent in charge of the El Paso office, stated, "It certainly seems like they've taken a page out of the Middle East [book]" (Bracamontes 2010). The cartels' use of these tactics presents an evolutionary change in Mexico's war and calls for increased vigilance on the US side of the border as the violence pushes north.

United States

Hezbollah operatives are here in the United States.

—Rep. Michael McCaul (KGTV News, San Diego, April 18, 2013)

Within the United States, there have been over thirty arrests of Hezbollah activists in the last five years based on Joint Terrorism Task Force investigations in Philadelphia, New York, Detroit, and San Antonio. From an operational standpoint, the organization's footprint in the United States is growing in size and tactical power; Hezbollah cells have attempted to obtain Stinger missiles, M-4 rifles, and night vision equipment in the United States (US Senate Committee on Homeland Security and Governmental Affairs 2012). Hezbollah is heavily engaged in intellectual property theft and other financial schemes in the United States and also has US citizen sympathizers willing to do some of its leg work.

In 2010, seven Florida men who owned an export business in Miami were arrested for falsifying paperwork and invoices and illegally shipping electronics such as Sony PlayStations and digital cameras to a shopping center in Paraguay for resale. The men falsified wire transactions, moving and hiding money illegally (FBI 2010). The managers of the mall gave a certain percentage of their earnings to Hezbollah, estimated in the tens of millions of dollars annually. And, in 2013, a former leader of a Hezbollah militia group, Wissam Allouche, attempted to secure a job and security clearance from the Department of Defense. Allouche is a Lebanese man who married a US Army officer in Germany and moved to San Antonio, Texas, in 2002. The marriage dissolved, yet he became a US citizen in 2009, became a contractor for the L3 Corporation, and worked in the Middle East as a linguist. He came up on the FBI's radar when applying for a sensitive government job. As the FBI investigated, he completed security clearance paperwork in which he lied about his previous connections to Hezbollah and the dissolution of his marriage. He also falsely claimed to be a US Special Forces officer during visits to Joint Base San Antonio-Fort Sam Houston and tried to date women from the post, possibly to gain access to sensitive information. Pictures of Allouche during his Hezbollah days were used in court, and it was revealed he was given an Arabic name by the terrorist group meaning "god of death" (US District Court, San Antonio 2014).

As it proves increasingly difficult to plant their members in society, all terrorist groups are using a new technique: recruiting US citizens. In August 2012, the State Department specially designated Hezbollah for its financial support of the Syrian regime. After decades of support from Syria, officials say Hezbollah is now "repaying its debt to Assad by providing training, advice, and extensive logistical support to the Government of Syria" (http://www.state.gov/r/pa/prs/

ps/2012/08/196335.htm). Hezbollah has stepped up efforts to elicit sympathizers to leave the United States and join the government's army in Syria, similar to the group's successful efforts to lure thousands of Eastern European Muslims into the fight. Interestingly, Americans may now be fighting Americans in Syria; US citizens have been recruited to support the regime as well as al-Qaeda extremist rebel groups. The FBI is worried the Americans fighting in Syria will return to the United States to carry out terrorist attacks on behalf of Hezbollah or al-Qaeda with their newfound skills (*Washington Post* 2014). These new techniques by Hezbollah and al-Qaeda either to plant agents in the United States or to recruit from the US populace are very worrying.

HAMAS

HAMAS is an acronym for the group's name in Arabic: *Harakat Al Muqawama Al Islamiyya* (Islamic Resistance Movement); *hamas* is also a word in itself meaning "zeal" or "enthusiasm." Hamas was founded in 1987 as an arm of Egypt's radical Muslim Brotherhood. The group's home base is in Gaza City, in the Palestinian Gaza Strip. Hamas has historically received support from Iran and from private donors, especially in Saudi Arabia and the Arabian Gulf region. It has also received funds from Palestinian expatriates in the United States and other countries. Many funds historically have been directed to Hamas through Islamic charity organizations, but this funding has slowed since crackdowns on terrorist financing following 9/11. Hamas hopes to establish an Islamic state in the West Bank and the Gaza Strip and its charter states: "Hamas regards nationalism as part and parcel of the religious faith. Nothing is loftier or deeper in nationalism than waging jihad against the enemy and confronting him when he sets foot on the land of the Muslims" (http://terrorism.about.com/od/groupsleader1/p/Hamas.htm). Historically, Hamas has called for the destruction of the state of Israel and refuses to recognize it.

Hamas routinely aims for soft targets in Israel. However, the group is not above using its own citizens as pawns in the battle. Independent reports give detailed evidence that Hamas used hospitals, schools, homes, and mosques to hide weapons and soldiers during the Gaza War, an Israeli military initiative from December 2008 through January 2009. At 25 miles long and 6 miles wide, with a population of 1.5 million, Gaza is the sixth most densely populated place on earth, providing a very complex battleground situation. The UN report on the war mentions the possible use of children, women, and the elderly as human shields by Hamas. Malam, an Israeli intelligence think tank, produced a report using declassified material such as videotapes, maps, and operational

plans recovered on the ground by Israeli Defense Forces (IDF) troops. The information indicates that Hamas hid IEDs in and around civilian homes and hospitals and a screen shot from a video taken from a helicopter appears to show the use of children and the elderly as human shields for soldiers engaged in operations. Of the 1,444 Palestinians killed in the offensive, approximately 340 were children. On July 8, 2014, in response to the death of three Israeli teenagers in the West Bank presumed at the hands of Hamas, the IDF launched Operation Protective Edge. In addition to massive missile strikes on the West Bank and in Gaza, the IDF conducted a ground operation to find and destroy Hamas tunnels. A ceasefire commenced on August 27th, with the death toll standing at over two thousand Palestinians and eighty Israelis killed. The intense bombing of houses and apartment buildings left approximately 30% of the Palestinian population homeless. Human rights violations on both sides of the conflict are being investigated by the UN. Certainly the collocation of Hamas with civilians has brought suffering to the Palestinian people and, as with previous engagements, approximately 90% of the deaths were civilian noncombatants, and 20% children.

Worrisome is the partnering of Hezbollah and Hamas operating in the same "space" in terms of benefactors such as Iran and Syria and financing activities in the triborder area of South America. Although the ideologies differ, the two groups are forming an increasingly strong partnership in the Middle East. For instance, during the December 2008 to January 2009 Gaza War, Hamas and Hezbollah maintained continuous communication in all phases of the conflict. During the battle, Hezbollah's influence on Hamas's tactics was apparent, with the group relying more on rocket attacks and less on suicide operations. Iranian sources report Hezbollah trained Hamas in military tactics used to attack Merkava tanks, the main battle tank employed by the IDF. A Hezbollah parliamentary official confirmed the tactical exchange (Berti 2009).

Hamas in the Western Hemisphere

Hamas sympathizers also raise funds in the United States through false charities. Holy Land Foundation for Relief and Development, of Richardson, Texas, had offices in three states and raised $13 million in 2000 alone. It was the largest Muslim charity in the United States and, although it claimed donations went to aid Palestinians, it was singled out for support of Hamas, mainly to the families of suicide bombers (US General Accounting Office 2003). Also, the American organization CAIR, the Council on American–Islamic Relations, was identified as a Hamas sympathizer.

International Terrorist Group	Past and/or propensity for hitting soft targets?	With intent to kill?	Reach into US?	Capability?
al-Qaeda, affiliates	Yes	Yes	Yes, both from foreign nationals and U.S. citizens	Yes
Hezbollah	Yes	Yes	Yes, operational cells and US sympathizers	Yes
Hamas	Yes	Possibly	Possibly, through US sympathizers	Maybe
FARC	Planning	Possibly	Possibly, through liaison with cartels and street gangs	Yes

FIGURE 3.2 Summary of international threat against soft targets.

SUMMARY OF THREAT

After discussing the international terrorist groups most likely to strike the United States, it is possible to assess the threat they pose to our soft targets as summarized in Figure 3.2.

REFERENCES

Armstrong, Jane and Colin Freeze. "Hapless Immigrant or Terrorist Threat?" (November 20, 2009). http://www.theglobeandmail.com/news/national/hapless-immigrant-or-terrorist-threat/article1204891/

Benjamin, Daniel. "Briefing on the Designation of Hezbollah for Supporting the Syrian Regime." US Department of State.

Benjamin, Daniel and Steven Simon. *Age of Sacred Terror.* New York: Random House, 2002.

Berti, Benedetta. "Assessing the Role of Hezbollah in the Gaza War and Its Regional Impact." *Terrorism Monitor* 7, no. 4 (2009). Published electronically March 3, 2009. http://www.jamestown.org/single/?tx_ttnews[tt_news]=34575#.VAWRamO9_7M

Boettcher, Mike. "South America's 'Tri-Border' Back on Terrorism Radar." CNN, http://articles.cnn.com/2002-11-07/world/terror.triborder_1_tri-border-israeli-targets-argentine-intelligence-documents?_s=PM:WORLD (2002).

Bracamontes, Ramon. "Experts: Car Bomb in Juárez Mimics Middle East Terrorist Tactics." *El Paso Times,* July 17, 2010.

Brafman, Ori and Rod A. Beckstrom. *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Portfolio Publishers, 2006.

Caldwell, Alicia A. "Car Bomb in Mexico Drug War Changes the Ground Rules." (2010). Published electronically July 17, 2010. http://www.guardian.co.uk/world/feedarticle/9178042

CNN. "Al-Shabaab Backed by Money for US." cnn.com/2013/09/29/opinion/bergen-shabaab-fundraising/ (2013).

Council on Foreign Relations. "Al-Shabab." http://www.cfr.org/somalia/al-shabab/p18650 (September 29, 2013)

FBI (Federal Bureau of Investigation). "Agroterrorism." http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/february-2012/agroterrorism/ (2012).

———. "Seven Charged with Illegal Export of Electronics to U.S.-Designated Terrorist Entity in Paraguay." News release, February 19, 2010, http://miami.fbi.gov/dojpressrel/pressrel10/mm021910.htm

Hesterman, Dr. Jennifer. *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups*. Boca Raton, FL: CRC Press, 2013.

Hoffman, Bruce. "Al-Qaeda Has a New Strategy." *The Washington Post*, 2010.

———. *Inside Terrorism*. New York: Columbia University Press, 2006.

Investigative Project on Terrorism. "Mexican Arrest Indicates Hizballah Seeking Foothold" (July 7, 2010).

Jones, Seth G. *Hunting in the Shadows: The Pursuit of Al Qa'ida since 9/11*. New York: W. W. Norton & Company, 2012.

KGTV News, San Diego. "House Homeland Security Chairman Tells Team 10 'Hezbollah in U.S.'" http://www.10news.com/news/investigations/house-homeland-security-chairman-tells-team-10-hezbollah-in-us

Levitt, Matthew. "Hizballah's Canadian Procurement Network." http://www.washingtoninstitute.org/uploads/Documents/opeds/Levitt20120813-2.pdf (2012).

Olsen, Matthew G. "Understanding the Homeland Threat Landscape." http://homeland.house.gov/sites/homeland.house.gov/files/Testimony-Olsen.pdf (2012).

Raghavan, Sudarsan. "Niger Struggles against Islamist Militants." *The Washington Post,* August 17, 2012.

Rotella, Sebastian. "Government Says Hezbollah Profits from U.S. Cocaine Market Via Link to Mexican Cartel." http://www.propublica.org/article/government-says-hezbollah-profits-from-us-cocaine-market-via-link-to-mexica (2011).

Sageman, Marc. *Understanding Terror Networks*. Philadephia, PA: University of Pennsylvania Press, 2003.

Senate Armed Services Committee. "Posture Statement, Commander, U.S. Southern Command," March 17, 2009.
Shekau, Abubakar and Josh Levs. "'I Will Sell Them,' Boko Haram Leader Says of Kidnapped Nigerian Girls." (May 5, 2014).
Spagat, Elliot and Jacques Billeaud. "Drug Tunnels Discovered between U.S.–Mexico Border Contained Railcar System, Tons of Pot " http://www.huffingtonpost.com/2012/07/14/drug-tunnels_n_1673317.html (2012).
Steele, Jonathan. "Bombers' Justification: Russians Are Killing Our Children, so We Are Here to Kill Yours" (2004).
US Department of State. "Assessing the Strength of Hizballah" (2010).
US District Court, San Antonio, Texas. "Sealed Indictment against Wissam 'Sam' Allouche." (2014).
US District Court, Southern District of New York. "Sealed Indictment: Jamal Yousef." http://www.fas.org/programs/ssp/asmp/externalresources/2009/Yousef,Jamaletal.S3Indictment.pdf (2009).
US District Court for the Eastern District of Virginia. "Sealed Indictment: Ayman Joumaa." http://www.investigativeproject.org/documents/case_docs/1856.pdf (2011).
US General Accounting Office. "Terrorist Financing: U.S. Agencies Should Systematically Assess Terrorists' Use of Alternative Financing Mechanisms" (November 2003).
US Military Academy. "Letters from Abbottabad: Bin Ladin" (2012).
US Senate Committee on Homeland Security & Governmental Affairs. *The Future of Homeland Security: Evolving and Emerging Threats* (July 11, 2012).
Washington Post. "FBI Director: Number of Americans Traveling to Fight in Syria Increasing," May 2, 2014.
Wright, Lawrence. *Looming Tower.* New York: Knopf, 2007.
Yaghi, Sobhi M. "Israel Is Preparing for War Tunnels and Hezbollah Elements in the Southern Syrian Border." http://www.aljoumhouria.com/news/index/15409 (July 2, 2012).
Zaboun, Kifah. "Gaza Tunnel Trade: Matter of Life and Death for Hamas." http://www.asharq-e.com/news.asp?section=1&id=30885 (August 31, 2012).

CHAPTER 4

Domestic Terrorism and the Homegrown Threat

Collateral damage.

—Timothy McVeigh, regarding the nineteen children killed in his attack

INTRODUCTION

Perhaps nothing is as hard to comprehend and explain as domestic terrorism. What motivates individuals to kill fellow citizens unremorsefully and target the very institutions providing for their safety and prosperity? Many of the drivers are the same as those found in international terrorism, such as an extreme religious or political ideology and the ability to find inspiration, encouragement, tactical techniques, training, and resources anonymously through the Internet. With domestic terror, lone wolves are of particular concern, inasmuch as they are already embedded in society and their clandestine activities are more difficult to predict and prevent. All of these factors make the detection and neutralization of the domestic threat extremely difficult for law enforcement agencies. Psychology is a factor, as well; the inherent disbelief in the phenomenon of domestic terrorism may result in a blind spot for investigators and first responders, a vulnerability best mitigated through education and training.

As a nation, we seem more transfixed by the threat of international terrorist groups striking on our soil, yet the number of domestic terror attacks has historically far outpaced international attacks against our citizens on our soil. Certainly the scope of violence differs, with international terrorist attacks typically having higher death rates and more property destruction than domestic events, with the rare exception of the Oklahoma City attack.

Since 9/11, we have engaged in two major theater battles in the Middle East resulting in thousands of US and coalition casualties,

simultaneously invoking the wrath of terrorist groups around the globe to attack our embassies and military personnel. All the while, we continue to fight domestic extremism at home, interrupting at least sixty radical terror plots on our soil (Zuckerman 2014). Clearly, securing our populace from the terror threat has evolved into an exhausting and complex situation for resource-constrained organizations, especially in light of ongoing fiscal stress. We cannot merely prioritize and address threats accordingly; each is significant and could be catastrophic to our country and its citizens. Terror groups can prey on this complex situation by fronting threats that may not exist (such as suitcase nuclear bombs), which forces us to spend billions of dollars on countermeasures and incite fear in the populace. A low-cost domestic scenario might be to set off a rudimentary improvised explosive device (IED) and claim it was a dirty bomb. Panic would ensue, and even if the government assured there was no radioactive material, it is likely that in the current environment of skepticism and a conspiracy-minded public, a sizeable portion of the population would not believe the statement. Playing on our fears can cause as much damage as a larger scale attack.

The definition of domestic terrorism has morphed since the events of 9/11 and subsequent attacks. Under current US law, set forth in the USA PATRIOT Act, acts of domestic terrorism are those which:

- Involve acts dangerous to human life that violate federal or state law;
- Appear intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination. or kidnapping; and
- Occur primarily within the territorial jurisdiction of the U.S.

Some legal experts point to the broad nature of these definitions, which could lead to the monitoring of innocent civilians and the erosion of freedoms such as free speech and the right to protest. Certainly, the balance between Constitutional rights and security is delicate and must be at the forefront of every discussion regarding the investigation and prosecution of all criminal activities. As the dangers and complexities associated with domestic terrorism continue to grow, so must our corresponding detection and mitigation activities to protect citizens from the rage of others.

HISTORY OF DOMESTIC TERRORISM IN THE UNITED STATES

There is a long list of domestic terrorist attacks in the United States, which some believe date back to the Boston Tea Party, fueling the

debate that "one man's terrorist is another man's freedom fighter." On December 16, 1773, a group of colonists called the "Sons of Liberty" disguised themselves as Native Americans, boarded British ships, and dumped cases of tea into the harbor as a sign of rebellion against the ruling government and its taxation laws. The attack prompted the passing of the Coercive Acts by the British, meant to contain and suppress rebellion among the colonists; however, they caused outrage and sparked the war for independence. Was the Tea Party freedom fighting or an attack against the state? As Bruce Hoffman points out, terrorism is difficult to define because the meaning of the term has changed so frequently over the past 200 years (Hoffman 2006).

To support the discussion of the persistence and lethality of modern domestic terrorism, we start in 1865 with the emergence of the Klu Klux Klan (KKK) at the end of the Civil War, marking the beginning of a new era of violence and unrest in our country. A secret vigilante group with extreme methods, the KKK violently murdered and intimidated African Americans and the white legislators who fought for their freedom from slavery and full integration into our society. The group routinely burned homes and bombed churches and schools with dynamite, in a campaign of killing and terrorizing. The KKK's attempts to keep black Americans from exercising their Constitutional rights such as voting led to the passing of the Civil Rights Act of 1871. The act banned the use of terror, force, or bribery by the KKK to prevent people from voting and made these and other terroristic activities federal offenses. The Klan continues to be an underlying current of hate in our country, with other white supremacists expanding the racist agenda to include anti-Semitism, such as Christian Identity offshoot Aryan Nations, which formed in the 1970s. Expert Bruce Hoffman (1988) considers the Aryan Nations the first "truly nationwide terrorist network in the U.S."

Violent anarchism has been present in the United States for almost 100 years. In April 1919, an anarchist group, the *Galleanists,* mailed thirty-six dynamite bombs to high-ranking officials, including the attorney general of the United States. Their delivery was intended for May 1, when Americans would celebrate the international labor movement; however, several bombs exploded early and their unique packaging led to the discovery and neutralization of the other devices. Not content with this operation, the group struck again on the evening of June 2, 1919, when large dynamite and metal slug bombs simultaneously exploded in eight US cities. The group was targeting government officials and judges who endorsed antisedition laws and had sentenced anarchists to prison. On September 16, 1920, a horse-drawn wagon bomb exploded on Wall Street in front of the J. P. Morgan bank, killing thirty-eight people. The device consisted of 100 pounds of dynamite and 500 pounds of cast iron weights. Although the incident was investigated for many

years, including by the fledgling FBI (Federal Bureau of Investigation) in 1944, no one person or group was ever officially charged with the crime. Continuing labor struggles and anticapitalist sentiment led by anarchist groups such as the violent Galleanists were likely at the root of this bombing. Anarchists are very active around the world, protesting and resorting to violent tactics as needed to spread their message. They are especially known for their blatant disregard for law and for their willful destruction of property.

Bath, Michigan, was the scene of a "lone wolf" soft target anti-government attack on May 18, 1927. Andrew Kehoe, upset with policies and tax law he believed led to his farm foreclosure, murdered his wife and then detonated three dynamite bombs at the Bath Consolidated School, where he worked as the treasurer. Kehoe spent months planting explosive material throughout the building in a premeditated act that stunned the country. When confronted at the scene by law enforcement, he detonated a vehicle bomb, killing himself and the school superintendent. In a similar act of rage eighty-three years later, software engineer Joseph Stack set his house on fire and then flew a small aircraft into the Internal Revenue Service building in Austin, Texas, which housed three hundred workers. Stack was furious about his tax problems and angry with collection agencies. His February 18, 2010, suicide note stated:

> Violence not only is the answer, it is the only answer and I saw it written once that the definition of insanity is repeating the same process over and over and expecting the outcome to suddenly be different. I am finally ready to stop this insanity. Well, Mr. Big Brother IRS man, let's try something different; take my pound of flesh and sleep well. The communist creed: From each according to his ability, to each according to his need. The capitalist creed: From each according to his gullibility, to each according to his greed. (CBS News 2010)

Stack's attack killed an IRS manager, seriously injured fifteen other workers, and cost the IRS $38 million to replace the building and its operation.

The 1960s and 1970s saw the rise of far-left violent antiestablishment groups such as the Weather Underground, a group formed at the University of Michigan, Ann Arbor, campus in 1969. The group held Marxist views of the elite ruling the middle class and bombed both the Pentagon and the State Department, as well as corporations. The Symbionese Liberation Army, which started as a black revolutionary group and grew into a violent guerilla-type organization, carried out robberies, bombings, and murders, once using hollow-point bullets packed with cyanide to kill a school superintendent and his deputy. The militant Black Panthers began with a socialist agenda but soon morphed into an antiestablishment group routinely targeting law enforcement. Spurred by anti-Arab and anti-Muslim ideology, the Jewish Defense

League (JDL) launched twenty-seven attacks against organizations it perceived to be anti-Semitic, including universities and academics. Black September, the Palestinian group responsible for the killing of eleven Israeli athletes at the 1972 Munich Olympics, was quite active in the United States, plotting to kill Prime Minister Golda Meir during a visit to New York City in 1973 with three pre-positioned car bombs, which failed to detonate. Political ideology fueled the Puerto Rican paramilitary group, the Fuerzas Armadas de Liberación Nacional (FALN), which was particularly brutal in its tactics and executed 120 bombings in the United States between 1974 and 1983, with targets including restaurants and a theater. The FALN was a Marxist-Leninist group wanting the United States out of Puerto Rico both militarily and politically.

Moving forward to 1978, the country was transfixed by attacks perpetrated by Theodore Kaczynski, a Harvard University graduate and former mathematics professor. Kaczynski was a self-professed "neo-Luddite," or one opposing modern technology who destroys private property as a means of protest. He lived in a wood shack in the forest, forgoing water or electricity; Kaczynski became enraged when developers moved into the area, destroying trees and displacing animals. Over the course of the next seventeen years, Kaczynski sent sixteen letter bombs to academics and others working in technological fields, killing three people and injuring twenty-three. Labeled the University and Airline Bomber (UNABOM) by the FBI, his lengthy manifesto was published in 1996 in the *New York Times* and the *Washington Post,* under the threat of more attacks. Kaczynski's campaign of terror against soft targets ended with capture when his brother recognized his work and called authorities.

On April 19, 1995, in the deadliest act of domestic terror in our country's history, Timothy McVeigh detonated a truck bomb in Oklahoma City, killing 168 people and injuring 680 others. Victims included children in a childcare center located with this government facility. McVeigh and coconspirator Terry Nichols met in the army, becoming antigovernment survivalists who supported the militia movement. McVeigh was likely aligned with the Christian Identity group and Nichols with the sovereign citizen movement. McVeigh was enraged with the government's handling of the 1992 Ruby Ridge, Idaho, standoff, as well as the 1993 Waco, Texas, standoff with the Branch Davidian religious sect. McVeigh visited Waco during the siege and after its tragic ending, when the compound caught on fire, killing seventy-five occupants including children. McVeigh stated the Oklahoma City bombing was retribution against the government for Waco. Prior to his death by lethal injection in 2001, McVeigh was housed in the same Supermax wing, known as "bomber's block" with Ted Kaczynski and al-Qaeda mastermind Ramzi Yousef. After the deadly Oklahoma City bombing, then-Attorney General Janet Reno formed a special task force to coordinate the country's response to the threat of domestic terrorism. The

task force was scheduled to hold one of its monthly meetings on September 11, 2001, but did not for obvious reasons. In fact, because the threat of jihadist terrorism has taken so much of the government's attention since 9/11, the special task force has never met again.

Eric Robert Rudolph, also an army veteran, was responsible for a series of deadly bombings between 1996 and 1998, killing two people and injuring over one hundred. His targets included Centennial Park at the Olympic Games in Atlanta, two abortion clinics, and a gay bar. Rudolph was a member of the Christian Identity movement, a white nationalist sect that believes God's chosen people are white and all others are condemned to hell. Although Rudolph claimed religious motivation and his antiabortion, antigay agenda for his attacks, he stated his actions were not racially motivated. He was on the run until 2003, when he was caught in a small North Carolina mountain town, rummaging through a dumpster and looking for food. After pleading guilty and apologizing to family members of those he killed and injured in the Atlanta attack (only), Rudolph avoided the death penalty and is serving a life sentence at the Supermax facility, just down the hall from Kaczynski and Yousef.

In 2009, an act of domestic terror occurred on a military installation at Fort Hood, Texas. Former Major/Dr. Nidal Malik Hasan, a man who took not only the oath to protect and defend our country, but also the Hippocratic oath to prevent harm to humans, stunned our country when he ambushed and killed thirteen of his fellow soldiers as they processed for deployment. Inspired to carry out his plan by radical Islamist Anwar al-Awlaki through a series of e-mails, Hasan voiced his extremist views and opposition to his upcoming deployment to Afghanistan to his chain of command prior to the shooting but no action was taken. Federal law enforcement agencies were aware of the communication between Awlaki and Hasan, yet the information was not passed to the base. On August 28, 2013, Hasan was found guilty of thirteen counts of premeditated murder and thirty-two counts of attempted murder and was sentenced to death. Being on death row has not changed Hasan's propensities; in August 29, 2014, he wrote a letter to the leaders of ISIS asking for "admittance" to the Islamic State.

THE TWENTY-FIRST CENTURY AND THE RISING TIDE OF DOMESTIC EXTREMISM

Of the sixty domestic terror plots, either successful or detected prior to execution, forty-nine could be considered homegrown terror plots, meaning one or more of the actors were American citizens, legal permanent residents, or visitors radicalized predominantly in the United States (Zuckerman 2014). The year 2014 started with a flurry of domestic terror

activity. On New Year's Day, National Guardsman intelligence analyst Andrew Scott Boguslawski, who held a top-secret clearance, was arrested for speeding on I-70 west of Columbus, Ohio, heading toward Indiana and his likely target—the Muscatatuck Urban Training Center. Boguslawski worked at the classified center, routinely used by special military and law enforcement units. After writing the speeding ticket, the law enforcement officer spotted what he thought was a gun between Boguslawski's legs and called for backup. This was a good thing: in all, Boguslawski had eighty-three explosive devices, including IEDs in five-hour energy bottles, two loaded pistols, an AR-15 sniper's rifle, and remote detonating devices. He also had the blueprints to the training facility.

In February 2014, three members of a Georgia militia were arrested and charged with conspiracy to attack federal agencies with explosive devices. They were attempting to obtain pipe bombs and thermite devices in order to carry out an attack on the TSA, FEMA, and other agencies. In May 2014, Todd Dwight Wheeler was arrested at his home on a sleepy cul-de-sac outside Washington, DC. His basement yielded 100 pounds of explosives plus hypodermic needles, constructed bombs, and a cache of weapons; his motives were unknown.

Unfortunately, there is no open-source government repository for information regarding the number and scope of domestic terror groups in the United States, perhaps by design. Other groups have stepped into the void: the Heritage Center with its tracking of domestic plots, but most notably the Southern Poverty Law Center (SPLC). The SPLC is a nonprofit civil rights organization "dedicated to fighting hate and bigotry, and seeking justice for the most vulnerable members of society." Founded in 1971, the organization has successfully prosecuted cases against white supremacist groups and other extremist organizations on behalf of its clients. Part of its mission is to "track the activities of hate groups and domestic terrorists across America," and many federal agencies are the benefactors of its vast repository of information. The groups tracked by SPLC include antigovernment, radical religious, neo-Nazi, Klu Klux Klan, Aryan Nations, black separatist, antigay, anti-immigrant, and the newest category, anti-Muslim groups. Some question the SPLC's methodology for labeling a group as "extremist" but its database is extremely valuable for tracking trend, tactics, and ideology.

The number of hate groups in the United States has steadily climbed in the last decade. In 2006, the SPLC reported 844 domestic hate and extremist groups; this number jumped to 939 in 2014. Hate-fueled incidents during the period of escalation include the 2009 killing of a guard at the Holocaust Museum in Washington, DC, by a self-proclaimed neo-Nazi; the 2010 bombing of a mosque in Jacksonville, Florida; the 2011 attempt to bomb the Martin Luther King parade in Spokane, Washington; the 2012 shooting at a Sikh temple in Wisconsin, killing six

worshippers; and the 2014 shootings at two Jewish community centers in Kansas City, Missouri, killing three.

Postmodern domestic terror is similar to international terror because groups are often loose coalitions and franchises, held together by ideology, rather than a strong and charismatic leader. According to radicalization expert Daveed Gartenstein-Ross, the most frequently cited work on the concept of "leaderless resistance" was published by white supremacist Louis Beam in his *Inter-Klan Newsletter & Survival Alert,* in 1983, and again in his journal, *The Seditionist,* in 1992. Beam believed the traditional hierarchical methods of organizing the white separatist left it vulnerable to destruction by the government; therefore, at some point, white separatists would not have the option of belonging to a group. He proposed a "leaderless resistance" structure, modeled after "committees of correspondence that existed throughout the thirteen colonies during the American Revolution." Beam postulated that each committee receive information from the government, but be a secret cell, operating independently, and that action be taken on a local level. He also proposed organization around "very small or even one-man cells of resistance" and advocated staying away from pyramidal organizations that are "an easy kill" for the government in light of federal informants and intelligence-gathering capabilities. "The last thing [f]ederal snoops" want, according to Beam, are "a thousand different small phantom cells opposing them" (Gartenstein-Ross and Gruen 2010).

Leaderless resistance, or the "phantom cell," has moved from the white supremacist realm into all other areas of domestic terrorism. By leveraging the Internet, groups can give tactical direction, guidance, inspiration, and money to followers, who then conduct operations independently. The anarchist magazine *Do or Die* explains:

> The North American ELF [Earth Liberation Front] has no central authority, no membership, no public meetings and no mailing lists. People from all walks of life are taking action as ELF activists, and this loose structure has created a network that is effective and very hard for state and industry forces to infiltrate and destroy. (Cecil-Cockwell 2008)

The leaderless resistance methodology also culls lone wolves from society and encourages and enables them to act. Therefore, an engagement strategy might be more effective if the ideology is countered than by trying to confront individuals or groups.

Domestic terror groups and incidents are often categorized as right wing, left wing, "single issue" and radical Islamist, or in this case, "homegrown." Although it is impossible to cover all groups in one mere chapter, most either have a history of attacking soft targets or the will to do so to further their goals.

RIGHT-WING EXTREMISM

Right-wing groups often adhere to the principles of racial supremacy and embrace antigovernment, antiregulatory beliefs. Right-wing terrorism is typically associated with those espousing neo-Nazi and racist ideologies, as well as opposition to foreigners and immigration. According to the FBI, in the late 1990s, right-wing extremism overtook left-wing terrorism to become the most dangerous domestic terrorist threat to the country. A joint 2013 report by the National Counterterrorism Center, the National Consortium for the Study of Terrorism and Responses to Terrorism, and the Southern Poverty Law Center found that right-wing extremists have been responsible for 56 percent of domestic terrorist attacks and plots since the 1995 Oklahoma City bombing (Sofer and Bernstein 2012). The Ruby Ridge confrontation and the Waco Siege cemented the right-wing faction and ideology in our country. Post 9/11, DHS believes hot-button issues such as immigration, gun control, abortion, and anti-Muslim sentiment, along with the election of the first African American president, present "unique drivers for right-wing radicalization and recruitment" per their controversial 2009 report. *Rightwing Extremism: Current Economic and Political Climate Fueling Resurgence in Radicalization and Recruitment* was a study crossing administrations by being completed in one and released in the next. The material was withdrawn by the DHS due to political backlash, but was certainly a significant piece of open source intelligence, rarely shared with the public. The authors also found that "lone wolves and small terrorist cells embracing violent right-wing extremist ideology are the most dangerous domestic terrorism threat in the United States." The report warned that groups might seek to recruit military personnel due to their access to bases, equipment, and tactical knowledge. "Returning veterans possess combat skills and experience that are attractive to right-wing extremists. The DHS/I&A team is concerned that right-wing extremists will attempt to recruit and radicalize returning veterans in order to boost their violent capabilities." Finally, the report controversially stated that returning veterans who were "disgruntled, disillusioned, or suffering from the psychological effects of war" would be vulnerable for recruitment (DHS 2009). This assessment was likely due to the involvement of several military veterans in previous attacks, such as McVeigh, Rudolph, and others, and proved to be quite prescient with the Fort Hood shooting and other violent incidents tied to current or former members of the US military. A quick online search provides proof that extremist groups are actively recruiting military and law enforcement to join their ranks. For example, a video entitled "2012 ALERT! An Open Message to Police and Military" is posted on several militia and antigovernment extremist websites, with hundreds of thousands of views.

Data gathered by several watchdog groups and think tanks supports the DHS report finding of the rise of right-wing extremism: 56 percent of domestic terrorist attacks and plots in the United States since 1995 have been perpetrated by right-wing extremists, as compared to 30 percent by ecoterrorists (left wing) and 12 percent by Islamic extremists (homegrown). In fact, right-wing extremism has been responsible for the greatest number of terrorist incidents in the United States in years since the Oklahoma City bombing (Sofer and Bernstein 2012).

Militias

By definition, a militia is a military force comprising ordinary citizens to provide defense and law enforcement without pay. The original militias were force multipliers during the Revolutionary War, protecting towns and citizens from the British army. However, modern militias are right-wing groups with paramilitary training that stockpile weapons and explosives and have a conspiracy-oriented ideology. The modern militia movement arose after the Waco and Ruby Ridge events, as members disagreed with the government's actions. Timothy McVeigh was aligned with the Michigan militia, which has the most active members in the country. Lee Miracle, a postal worker who goes by the moniker "Weapon M" has his own webpage and participated in an interview with a major news network showing his young daughter expertly handling a shotgun. Although Miracle is a moderate in the militia realm, advocating for his troops to stockpile and prepare for a homeland defense mission, most militia websites are replete with paranoid, antigovernment rhetoric and warnings about a dark future filled with disasters, calamity, and FEMA "concentration camps" that are currently under construction. Also, a member of the Michigan Militia, Mark Koernke, served a three-year prison sentence for assaulting a police officer and resisting arrest. Upon return to society, he started the Liberty Tree Radio station and a series of webcasts. Programs like Koernke's and videos on the Internet, both protected by the First Amendment as free speech, further spread conspiracies about forthcoming martial law and a crackdown by the "new world order."

There are almost 100 militia groups in the United States with an overarching, harmless sounding motto to "protect the Constitution against all enemies, foreign and domestic." However, their definition of a "domestic enemy" is worrisome and can include government leaders they believe are sapping rights and freedoms. For instance, militias see healthcare reform and any type of gun control as unconstitutional. There is a long list of orders they refuse to follow, many of which could bring them weapon-to-weapon with law enforcement

and our military during states of emergency. The Oathkeepers, a group formed in 2009, has been linked to the militia movement. A prominent Oathkeeper (http://www.lincolncountywatch.org/links.html) stated openly: "The greatest threat we face today is not terrorists; it is our federal government"—a declaration becoming a mantra for members of right-wing extremist groups. Militias are not opposed to carrying out violent acts against soft targets to further their goals. For example, the Hutaree, a Michigan militia that was also part of the Christian Patriot movement, prepared for what they believed would be an apocalyptic battle with the Antichrist, who would be supported and defended by law enforcement. Their plan was to kill a law enforcement officer in March 2010 and then stage an attack on the officer's funeral procession and kill many others (US Department of Justice 2010). Despite hundreds of hours of video showing training and exposing the group's ideology and plans, seven of the nine convictions were overturned in court with the judge stating the prosecution failed to make its case. Two group members served two years on weapons charges.

Sovereign Citizens

According to a 2014 study conducted by the National Consortium for the Study of Terrorism and Response to Terrorism (START), which surveyed 364 officials from 175 law enforcement agencies, America's top perceived domestic terrorist threat is the sovereign citizen movement (START 2014). The group is unusual in its tactics, ranging from white-collar crime to impersonating and killing law enforcement officers. Experts believe the group has over 100,000 core and 200,000 fringe members and has been operating in the United States for at least 20 years (McNabb 2010). A spinoff of the defunct, violent Posse Comitatus, a white-supremacist, anti-Semitic group from the 1980s, the group's most famous member is Terry Nichols, who conspired with Timothy McVeigh to destroy the Murrah Building. The sovereigns' ideology has changed through the years, first believing "God gave America to the white man" and espousing conspiracy theories regarding Jewish control of the government. The group has moved away from this ideology, now believing it can operate outside any government authority. Therefore, its members do not adhere to laws or pay taxes. The group also believes in the "redemption theory," certain that the US government went bankrupt when it abandoned the gold standard basis for currency in 1933 and began using citizens as collateral in trade agreements with foreign governments. This notion fuels the sovereigns' belief that the government does not act in the best interests of its citizens and gives permission to steal from the US Treasury rightfully to secure money with the people.

Sovereigns also create and sell fraudulent documents such as driver's licenses, diplomatic and law enforcement credentials, and concealed firearms permits. The sovereign citizen Declaration of Independence states (grammatical errors included):

> We the People inhabiting the North American continent, free men and women convened under God, having been granted by the Creator dominion over all the earth, to restore the blessings of liberty for ourselves and the posterity, do hereby invoke our sacred right to alter or abolish destructive government as memorialized in The unanimous Declaration of the thirteen united States of America, c. 1776 by declaring herewith this solemn declaration to the people of the earth and all governments and nations derived there from.

Any confrontation with law enforcement is likely to end in violence. Since 2000, group members have killed eight law enforcement officers, wounding several others. In 2010, two Arkansas police officers stopped sovereign citizen extremists Jerry Kane and his sixteen-year-old son during a routine traffic stop on Interstate 40. Joseph Kane immediately jumped out of the vehicle and opened fire with an AK-47 assault rifle, instantly killing both officers. In 2011, sovereign citizen James Michael Tesi shot a police officer in Texas on a traffic stop; the officer survived. In 2012, Sheriff's Deputies Brandon Nielson and Jeremy Triche were ambushed and killed at a trailer park in La Place, Louisiana, while investigating an earlier shooting in which two deputies were shot and wounded working a traffic detail. A SWAT team entered the trailer park and apprehended the group—four men and three women, some with ties to the sovereign citizens and others with criminal records. The group had been under surveillance in Tennessee and then De Soto Parish, Louisiana, after brushes with the law including weapons charges, high-speed chases, and having sovereign citizen's paraphernalia. Unfortunately, the group left law enforcement radar just a few weeks prior to the shooting, moving to La Place (Galofaro 2012). Although an official investigation report was never released, information was likely not shared between federal and local law enforcement, creating an ambush situation for the officers.

Sovereigns have also engaged in elaborate planning to kill law enforcement and government officials, as well as their families. For example, in 2011, five people, including popular activist Schaeffer Cox, were arrested in Fairbanks, Alaska, for conspiring to kill multiple Alaska state troopers and a federal judge, his children, and grandchildren in what is labeled the "241" murder conspiracy case. The group stockpiled grenades and weapons with silencers and conducted surveillance on the homes of their targets. The five faced several state charges,

including conspiracy to commit murder, conspiracy to commit kidnapping, conspiracy to commit arson, and tampering with evidence, according to troopers. All pled guilty and were convicted, with Cox receiving a 26-year sentence (Burke 2012).

Cox, who unsuccessfully ran for Congress in 2008, had been on law enforcement's radar since 2009 as the leader of the Alaska Peacemakers Militia and the Second Amendment Task Force. He organized multiple gun-rights and personal freedoms rallies and was a member of a "Liberty Bell network," which sends out mass notifications to assemble a crowd of witnesses when a member believes his or her rights are being violated by the police. Cox's video repository can still be viewed online, and it serves as a great education tool for the mindset of a sovereign citizen, the conspiratorial nature of this ideology, and the willingness to use violence to "kill in the name of liberty" (The Solution: Schaeffer Cox Speaks on the Future of the Liberty Movement 2012).

Sovereigns may be identified through the following behaviors (FBI 2011):

- Using the terminology "freeing money from the strawman," a reference to the redemption theory and the US Treasury
- Names spelled in all capital letters or with colons (e.g., JOHN SMITH or Smith: John)
- Signatures followed by the words "under duress," "Sovereign Living Soul" (SLS), or a copyright symbol (©)
- Signing in red crayon on personal seals, stamps, or thumb prints in red ink
- The words "accepted for value"
- Presenting false identification, especially driver's licenses

Sovereigns not only have an inherent distrust of law enforcement, but also step up and engage, and then videotape, analyze, and share the officers' response. Sovereign Cop Watch, which has a branch specializing in "undercover and reverse sting police conduct investigations," has a strong presence on the Internet. Although its home website moves, the Facebook page is static with over 1,100 connections, and directs users to the updated homepage (http://www.facebook.com/sovereign.copwatch). The newest version includes a series of videos instructing members on how to resist arrest and manipulate law enforcement situations in order to win in court ("Steps to Sovereignty": http://flag-book.com/3-2-training-landing).

Sovereign citizens present a complex and dangerous challenge for law enforcement and society. Training and recognition of the groups' culture and tactics, as well as information sharing between agencies and states, is critical to engaging and mitigating the threat.

LEFT WING

Left-wing groups typically possess a revolutionary socialist doctrine, viewing themselves as the protectors of the people from capitalism and imperialism; however, they are willing to attack soft targets and kill citizens to further goals. Left-wing activism in the United States was spurred by anti-Vietnam sentiment, the perception that law enforcement was spying on citizens, and events such as the shooting of students at Kent State by National Guard personnel in the 1970s. These events caused government distrust, which led to protest and violent clashes. Leftist extremists were responsible for a preponderance of the domestic violence in the 1960s and 1970s and for three-fourths of the officially designated acts of terrorism in America in the 1980s. The United States was not the only country facing a strong threat from the left; internationally, of the 13,858 people who died between 1988 and 1998 in attacks, 74 percent were killed by leftist organizations. The threat from the left in the United States diminished in the 1980s and 1990s, as a result of the arrest of many group leaders and the loss of support from nations formerly affiliated with, or part of, the Soviet Union. However, the danger from the left remains formidable, especially from anarchist and single-issue activists.

Anarchists

Anarchism is a political philosophy that considers the State undesirable, unnecessary, and harmful, and instead promotes a stateless society, or anarchy. An anarchist is an individual who furthers his or her political and/or social goals through force or violence and violation of law. They may typically espouse anticapitalist, antiglobalization, communist, Marxist, and socialist philosophies. There are branches of the movement with specific agendas such as left, green, free market, and people of color. Anarchists promote a system called agorism, or revolutionary market anarchism. In a market anarchist society, law and security would be provided by market actors instead of political institutions.

Anarchists are now present at nearly every international gathering and they escalate fear among attendees, residents, and business owners, driving up security costs. For instance, Canada spent $900 million to secure Toronto for the G-20 summit in 2010, but it was not enough to keep anarchists from wreaking havoc on the streets, burning police cars, smashing storefronts, and terrorizing citizens. Those arrested were not just Canadians; anarchists from the United States and European countries traveled to the summit location to participate in the violence. Anarchist groups continue to use the black bloc technique, which

originated in German riots in the 1970s in which protestors wore black hoods, balaclavas, and helmets as a show of solidarity and as disguise. After the violent acts are perpetrated, the clothing can be stripped off so that the anarchist will blend in with other citizens and escape.

Anarchists are now moving beyond protests at events to actively planning attacks. In 2011, an anarchist group was arrested by the FBI for a plot to blow up a bridge in Cleveland, Ohio, using C-4 explosive. The attack was meant to bring down financial institution signage on the bridge, not necessarily the bridge. This event served as a good reminder about target selection not always being what it appears; had the bridge fallen due to the attack, the investigatory process may have leaned toward a homegrown terror theory and away from the true perpetrators and their rationale.

The anarchists regularly use Twitter to give real-time directions about where to rally, what to wear, and how to engage law enforcement and also extensively use websites and chat rooms to communicate, educate, and coordinate protests. When Los Angeles transit police officer Johannes Mehserle shot and killed Oscar Grant early New Year's Day, 2009, the anarchist community vigorously protested. Their activity escalated on July 8, 2010, when Mehserle's court case came to an end with a verdict and sentence. While monitoring anarchist websites and Twitter, I captured the following communiqué:

> To everyone coming out to 14th and Broadway on Verdict Day: Some of us will be with you at 14th and Broadway on the day of the verdict. We know that the pigs will be looking to cause trouble, but we're not going to give them an excuse. We want everyone in Oakland to come out to 14th and Broadway. We'll leave it to the will of the people assembled to decide what goes down there. Also, we just heard that Alameda County dropped at least $675,000 on an LRAD 300X sonic weapon system, so bring earplugs.

The communiqué indicates the very essence of leaderless resistance and the ability of the group to gather inside information and adapt operations based on law enforcement's posture.

The establishment of the Center for a Stateless Society (CSS), an anarchist think tank, has brought a group of academic elite to the table. CSS has a staff and advisory panel of experts, including professors from large universities, and also collects donations for its cause. The website includes a 106-question quiz to identify social and political "philosophy," and there is a large repository of well-written articles on anarchy (http://c4ss.org). The lesson CSS teaches is that we should not envision anarchists as mere thugs, storefront smashers, and "occupiers." Some of our academic elite believe in a stateless society and are in a position to compel others. A new organization, the Students for a Stateless Society,

recently launched its webpage with ideas for events from bake sales to protests; seven universities currently have chapters (http://s4ss.org/).

After 9/11, some American anarchists joined the ranks of the "truthers," who developed conspiracy theories about the attacks, including that the World Trade Center contained bombs, the Pentagon was hit with a missile, Israel was behind the attacks, or the event was an inside job done by the CIA. The Boston Marathon attack has been dissected frame by frame on the Internet by truthers who believe it was a false flag event staged by the government with actors, moulage, and props. Some even believe the attack at Sandy Hook elementary was a government-staged false flag operation. In terms of the larger threats to our country, it is interesting that American anarchists give little or no thought to 9/11, actively attempting to devalue the event and its impact on our country and world. The only significance they see is in how follow-on laws such as the PATRIOT Act impacted their cause. For instance, consider the following quotes from a recent document entitled "Ten Years after 9/11: An Anarchist Evaluation" (*Anarchist Developments* 2011):

- Anarchists, I argue, were among the few radicals whose analysis of history and power was not transformed, directly or indirectly, by the events of 9/11.
- A host of obvious questions accompany an attempt to encapsulate an event such as 9/11 and the ten years that followed, foremost among them: Why situate 9/11 as a date of exceptional importance? Does a reflection of this kind merely contribute to, for example, neoconservative attempts to enshrine 9/11 as a propagandistic tool? The response of the US government (and capitalist states worldwide) to 9/11 diminished the capacity of anarchist social movements through a barrage of draconian laws, militarization of police forces, and repressive new forms of technological surveillance.
- In a discussion about the "We Will Never Forget" slogan, the counterproposal is "The Forgetful Memory of 9/11."

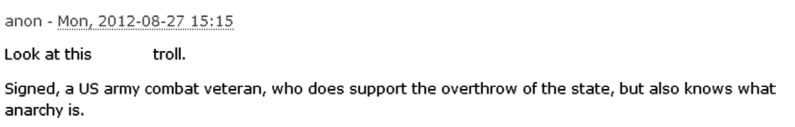
While accomplishing research for an article on anarchism, I participated in an online chat anonymously with self-professed anarchists. We were discussing terrorist threats from al-Qaeda and other groups, and most participants did not perceive any kind of danger at all, believing the government has overblown the situation to justify military activities abroad and additional policing activities in the United States. I mentioned the overarching goal of extremists who want to turn the United States into an Islamic republic under Sharia law. One of the participants stated he would "rather see the flag of any group or country flying over our Capitol than the flag of the US," and several others piled on with

their concurrence. I found this discussion extremely shocking and worrisome, but not because these opinions are provocative or different from the mainstream. The concern arose from the perspective of anarchists being hyperfocused on an ideology to the point where they do not perceive outside threats and exclude the possibility they may exist, or that they, as Americans, are in the crosshairs. Furthermore, in terms of liaising with international or domestic terror groups, although this is not a goal of anarchists, the groups do all share a common enemy: the government—*any* government.

Anarchism and the Military

The increasing number of ex-military members posting on anarchist blogs is also something of interest; they typically receive a warm welcome and of course bring a host of expertise to the table for the movement (Figure 4.1).

The case of US Army PFC Michael Burnett and his three accomplices allows insight into a case of anarchism and dissension within the active military ranks. Their domestic terrorism plot was revealed during the investigation of the murder of PFC Michael Roark and his girlfriend, who were executed by the group on December 4, 2011, as "loose ends" who knew about their plans and were going to warn authorities. On August 27, 2012, Burnett testified about the plot to overthrow the government as part of a US military anarchist/militia group called FEAR: *Forever Enduring Always Ready*. FEAR spent almost $100,000 on equipment, firearms, and property—money taken from the life insurance policy of the deceased pregnant wife of one of the group's members (her death is now under investigation as a possible murder). FEAR plotted to take over its home station, Fort Stewart, Georgia, and then bomb targets in Savannah, Georgia, including the Forsyth Park fountain. They also wanted to destroy a dam in Washington state and poison the apple supply. Group members had matching tattoos resembling an anarchy symbol. The ultimate goal of FEAR was to assassinate President Obama and "give the government back to the people" (Bynum 2012). The group members are serving prison terms ranging from thirty years to life without parole.


anon - Mon, 2012-08-27 15:15

Look at this troll.

Signed, a US army combat veteran, who does support the overthrow of the state, but also knows what anarchy is.

FIGURE 4.1 Post from a popular anarchist forum.

SINGLE-ISSUE OR SPECIAL-INTEREST TERRORISM

Single-issue or special-interest terrorism is a brand of extremism different from right- and left-wing terrorism, as groups try to influence specific issues, rather than to affect political change. Actors are on the extreme fringes of animal rights, environmental protection, pro-life, and antinuclear movements, attempting to sway public opinion in their favor. Thirty percent of all domestic terror attacks since 1995 were related to special-interest terrorist groups (Sofer and Bernstein 2012). A difficult extremism to comprehend, group members often believe it is justifiable to kill a human being in the name of saving an animal, a tree, or an unborn child. Groups typically operate underground, with no hierarchy. They are basically leaderless with small cells around the world, and the ideology (as well as the Internet) serves as the glue for the cause. Thousands of acts of violence and property damage in the last ten years have been attributed to special-interest terrorism. Leslie Pickering, a spokesperson for ELF, explains how acts of violence help draw attention to a cause: "The whole time I was protesting, nobody cared. The whole time I was writing letters, nobody cared. The whole time I was doing civil disobedience, nobody cared except for the media. But all of a sudden, when buildings were blowing up, a lot of people cared" (Cecil-Cockwell 2008).

The Earth Liberation Front

According to its press office, ELF uses "economic sabotage and guerrilla warfare to stop the exploitation and destruction of the environment." This activity is also known as "ecotage." Originating in the United Kingdom in 1992, ELF's first activity in the United States occurred in 1996, when the group spray-painted buildings and used glue to damage locks on McDonald's restaurants in Oregon. Their activities quickly escalated; in March 2001, the FBI classified ELF as the top domestic threat due to a string of arsons destroying a ranger station, large houses, and a Land Rover dealership, as well as the firebombing of a lab at Michigan State University. The group was active throughout the next decade, destroying a 206-unit condominium complex in San Diego in 2003, and four multimillion-dollar homes on Seattle's "Street of Dreams" in 2008. Oddly enough, the Street of Dreams homes were "green" and the emissions from the ELF fire did far more environmental damage than the homes would have in 100 years. The group seems to be diminishing over time; however, it could still pose a threat.

IN FOCUS: AGROTERRORISM—A SOFT TARGET ATTACK

The agroterror threat is not given as much weight as other dangers, for instance, WMDs weapons of mass destruction. However, as terror groups increasingly realize striking the economic structure is a powerful means to get attention and concessions, the possibility of an asymmetric, soft target attack to the food supply is escalating. Also, as other avenues of attack are closed down or increasingly difficult to navigate, agroterrorism may seem an increasingly attractive alternative and its impact would be felt across the population.

The quarantine of stock, the economic loss to farmers, and the international impact of sudden withdrawal from the food market would likely cause the fear and economic loss sought by terror groups. Also, this type of attack is relatively inexpensive compared to other operations, making it all the more attractive. Experts believe foot and mouth disease (FMD) is the most likely and pressing threat. Although eradicated from our country, FMD can still be found on other continents and is extremely contagious, with humans able to carry the virus for up to forty-eight hours. The virus can travel fifty miles to affect other herds and persists for weeks on cloth and in straw. Our "megafarms" with ten thousand head of cattle are especially vulnerable targets to FMD. The impact of FMD on the economy was experienced in Great Britain in 2001, when nine thousand farms were infected, leading to the slaughter of over four million animals. Naturally, this type of mandatory process would also anger animal activists and likely lead to their uprising.

Another type of attack, with bacteria such as botulism, *Escherichia coli,* and salmonella, could be launched against packing plants. The 2008 case of salmonella contamination at the Peanut Corporation of America (PCA) sheds light on the vulnerability of the packing industry. PCA peanut butter and peanut meal were used in 3,919 products manufactured by 361 companies, and the recall related to the contamination was the largest in US history. The sale of all peanut butter dropped 25 percent as scared consumers avoided the product completely. At least nine people died and over 714 were sick as a result of salmonella; the most vulnerable members of society to this type of poisoning are children, the elderly, and those with compromised immune systems. The fruit and vegetable supply chain is possibly the most vulnerable, with the least amount of bioterrorism protection measures in place, and little to no processing with bacteria killers such as heat.

A major problem with investigating these types of issues is state and local law enforcement have jurisdiction. Establishing the adequate quarantine upon detection, consisting of hundreds of square miles and possibly crossing state lines, would be difficult to enact without federal oversight. The same holds true for stopping trucks and trains with contaminated cattle or food in transit throughout the country. Resource-constrained departments would be stretched to the limit responding to such a disaster. The FBI emphasizes the theft of vaccine-, medicine-, and livestock-related equipment must be reported and is of concern from a national security perspective. Certainly, local and state inspectors and law enforcement must take care to gather evidence and assume a mass outbreak or contamination could be the work of terrorists.

Finally, the PCA case also shed light on the seasonal workers employed at packing plants, typically an unscreened transitional populace. Lack of preparedness is a weakness the enemy seeks to exploit; therefore, our training and vigilance are paramount to protecting our agriculture industry from an agroterror attack (Primary source: Olson, February 2012)

Animal Liberation Front

Members of the Animal Liberation Front (ALF) see themselves as the liberators and rescuers of animals. Also, a primary goal is to inflict economic damage on those who profit from the misery and exploitation of animals. ALF's roots are in the United Kingdom, dating as far back as 1976; it appeared in the United States in 1982. Early ALF activities identified illegal animal research and resulted in legal action against the perpetrators of the crimes; however, ALF abroad became violent in the 1980s, sending letter bombs to government leaders. The group then began to engage in elaborate hoaxes, claiming to have poisoned food products and cosmetics and costing companies millions of dollars in recalls, product destruction, and lost customers. Fur companies were firebombed, and devices were planted on executives' vehicles and at their doorsteps. This brand of violence moved to the United States in the 1990s and grew in intensity, with a string of incidents leading to injuries to innocent bystanders and millions of dollars in property damage.

On January 20, 2006, as part of Operation Backfire, the US Department of Justice announced charges against nine American and two Canadian activists calling themselves the "The Family." At least nine of the eleven pleaded guilty to conspiracy and arson for their role in a string of twenty fires from 1996 through 2001; damage totaled $40

million. The Department of Justice called their activity domestic terrorism, with incidents including arson attacks against meat-processing plants, lumber companies, a high-tension power line, and a ski center in Vail (US Department of Justice 2006). Environmental and animal-rights activists have referred to the legal action by the government as the "green scare," and the roundup does not seem to have deterred the groups. ELF has been somewhat quieted, but ALF has stepped up its efforts, breaking into farms and liberating exotic animals, hacking websites, sabotaging race tracks, and burning meat trucks. Its press office website, which has a section with pictures of federal agents who investigate the group, as well as "snitches and informants," instructs followers:

> Talking to law enforcement will always hurt you and others. The Feds or the local police are not your friends no matter how much they ensure [*sic*] you that they are trying to help you. Law enforcement will always resort to fear and intimidation and we must resist such divisional tactics. (NAALPO n.d.)

A favorite quote among left-wing groups is, "Snitches get stitches, and end up in ditches."

In terms of future operations, ALF ideology could certainly be in line with attacks against the food supply in our country. Many experts believe they would easily liaise with other terror groups to further each other's goals and bring attention to their disparate causes.

HOMEGROWN TERROR

> Our long-held belief that homegrown terrorism couldn't happen here has created a situation where we are today, stumbling blindly through the legal, operational, and organizational minefield of countering terrorist radicalization and recruitment occurring in the U.S.
>
> **—Bipartisan Policy Center (2010)**

At least sixty domestic terror plots have been identified, mitigated, or failed since the tragic events of 9/11. Some are more memorable than others: Richard Reid, the shoe bomber; Jose Padilla, the dirty bomber; the Lackawanna Six; the Fort Dix plot; the LA Airport "Doomsday" plot; the Raleigh jihad group; Najibullah Zazi's backpack plot against the NYC subway; Shahzad, the Times Square bomber; and Abdulmutallab, the underwear bomber. Other homegrown plots since 9/11 include the planned or attempted bombing of buildings, bridges, and landmarks, and the targeting of malls, railroads, and subways. The Heritage Foundation has compiled a thorough list of disrupted domestic attacks since 9/11

and it is worthy of review as a reminder of the breadth, depth, imagination, and scope of our homegrown terrorists (Zuckerman 2014). Since 1995, 12 percent of the domestic terror cases in the United States were perpetrated by Islamic extremists (Sofer and Bernstein 2012).

Perhaps the most glaring evidence of our blind spot to the domestic radical Islamist terror threat is that, besides the occasional white paper or webinar, our own country's think tanks are doing very little data collection and analysis on the issue. The Henry Jackson Society think tank in the United Kingdom spent years analyzing US challenges and issued a 700-page report entitled: *Al-Qaeda in the United States: A Complete Analysis of Terrorism Offenses,* by Robin Simcox and Emily Dyer (2013). The preface was written by the former director of the CIA, General Mike Hayden. I attended the book unveiling in Washington, DC, in 2013, which was moderated by General Hayden, and was stunned to hear the statistics compiled by the researchers. The publication provides a comprehensive analysis of 171 al-Qaeda and al-Qaeda-inspired terror convictions in the United States between 1997 and 2011. Profiles of those who committed these al-Qaeda-related offenses (AQROs) are included, and the report contains a statistical breakdown and analysis of key trends, including nationality, age, occupation, percentage of religious converts, education levels, type of charge, the role of each individual offender, connections to terrorist networks, whether terrorist training was undertaken, place of residence, and whether the individual had combat experience.

Major report findings include (Simcox and Dyer 2013):

Demographics

- 95% of offenders were men
- Age at the time of the charge was 19–63
- Almost a third were between the age of 20 and 24
- 36% were born in the United States, citizens; 18% were naturalized citizens; 46% were in the country on visas or expired visas
- 82% of offenders were living in the United States

Religion

- 23% were religious converts to Islam; all of those born in the United States were converts and all were converts from Christianity
- 95% of all convert offenders were US citizens

Employment and schooling

- 44% were employed; 20% in blue collar jobs
- 52% were college educated
- 23% had either graduate or doctoral degrees
- 13% were students

Plot type and training

- Of the 171 offenders, 63 were active participants plotting operationally large-scale attacks against the United States; 43 were aspirants; 36 were facilitators taking care of administrative and logistics support; 26 were trained aspirants; 3 were ideologues
- 57% of individuals were linked to a designated foreign terrorist organization (FTO); 38% were linked to al-Qaeda or an al-Qaeda-inspired group such as Lashkar-e-Taiba or al-Shabbab
- There were 36 mass casualty operatives (MCOs) planning 10 attacks in the United States to cause mass loss of life
- 47% of all individuals had received terrorist training. Afghanistan and Pakistan were the main countries where this took place; of US citizens, one-third had received training
- 11% of individuals had received no training at all
- 47% of offenders had received training in formal terrorist camps in the United States
- 18% of offenders had combat experience
- 87% of combat trained offenders were directly linked to an FTO
- 50 of the cases were cracked during an undercover investigation; however, these were mostly aspirants, not active plotters

Often the plots by US citizens against their own country are elaborate, well constructed, and close to execution when detected. I unknowingly stood in the very spot in East Potomac Park where Rezwan Ferdaus, a US citizen from Ashland, Massachusetts, with a degree in physics, planned to launch a remote-controlled aircraft packed with 25 pounds of C-4 plastic explosives to attack the Pentagon in 2011. Following the initial strike, Ferdaus hoped to use six people, pre-positioned in the Pentagon parking lots and armed with AK-47s, to shoot into the crowd of panicked building evacuees. He acquired one of the aircraft through a PayPal account under a false name—a six-foot-long drone, capable of flying up to one hundred miles per hour. While planning this attack, Ferdaus also rigged IED detonators and gave them to FBI agents he believed were al-Qaeda operatives who would deliver them downrange for field testing. He was pleased to learn from agents that his first detonator "killed" American soldiers. After Ferdaus's arrest, scientists tore the plot apart, detailing for the press exactly why it would not have worked based on his selected radio frequencies and the weight of the C-4 load. They corrected the specifications, feeding the data to future plotters, no doubt. Also, there was so much rhetoric about the improbability of such an attack that the very essence of the operation was lost: it was creative, asymmetric, and plotted by a fellow citizen. Ferdaus was determined to kill Americans and attack what he called the "great Satan," his own country of birth.

The number of disrupted plots in our country is on the rise, meaning there are potentially many other undetected would-be terrorists or terrorist

cells operating off the grid. Radicalized Americans are typically educated, like Ferdaus. Leveraging the Internet, they move quickly along the continuum from contemplation to planning to execution. They are creative and highly adaptable, learning from failed operations. For example, when the Times Square bomber Faisal Shahzad ran away from his vehicle, leaving a smoking dud for a bomb, he was chastised by his handlers for failing to stay and work on the device until it exploded, and internal al-Qaeda correspondence indicated this doomed scenario would never happen again. The enemy is watching and learning; there is no such thing as a failure, only a stumbling block on the path to perfection. Unfortunately, our culture is hyperfocused on the last attack or attempt and fails to look forward, but terrorists continue to progress in methodology and target selection. They go on surveillance missions and measure the number of people and cars passing by and the distance from weapon to target. They probe and accomplish dry runs, perfecting the plan. Our very public "celebration" over a disrupted plot should be tempered by the thought that the next bomber is American and sitting in his or her home tonight, watching the same newscast, devising new and improved ways to kill us and destroy our way of life.

Not much time is spent contemplating what happens after the domestic terrorist is arrested. Few, if any, receive the life sentences given to Reid, Padilla, and Zazi. Most sentences are between 3 and 20 years, and the long periods of time spent in jail awaiting the court case are typically awarded as time served and deducted from the length of the sentence. As a result, many domestic terrorists and conspirators convicted since 9/11 have already served their prison sentences and were quietly released back to society. Those released include members of the Lackawanna Six and Portland Seven terror groups who traveled to Afghanistan for training with the Taliban and met bin Laden. Many other Americans convicted on terrorism charges are set to come out of prison in 2014, yet we have no plan for their rehabilitation and reintegration into our neighborhoods. Reradicalization is possible, perhaps with a renewed fervor due to anger projected toward the government. With the spread of al-Qaeda affiliates around the world and an increasingly disenfranchised population, the radicalized homegrown threat will, at the very least, remain constant, but is likely to rise.

Rehabilitation and the Domestic Terrorist

> A terrorist is only temporarily neutralized by imprisonment.
>
> **—Dennis Pluchinsky (2008)**

A few years ago, I was approached by the editors of *The Counter Terrorist Magazine* to write an article on jihadist recidivism—those who

leave prison and return to a life of terror—for the April/May 2010 issue (Hesterman 2010). I found an extraordinarily small body of research on the topic, despite the pressing nature of the problem. The list of former Guantanamo Bay detainees who are assuming leadership positions in al-Qaeda offshoots continues to grow, and jihadist recidivism is a persistent and growing feeder of manpower to international and domestic terror groups and operations. Also, recidivism provides a valuable resource to terrorist groups: experienced jihadists who have gained firsthand insight into enemy counterterrorism practices and agents through their arrest, sentencing, and detainment.

Capturing a terrorist is a resource-intensive event, and taking an enemy combatant off the battlefield and out of our neighborhoods is clearly a victory. However, the process must not end with the arrest, or even conviction; apprehension is merely the tip of the iceberg. Perhaps an even greater investment must be made on activities occurring during a prisoner's incarceration, rehabilitation, and release to ensure the jihadist remains permanently out of the fight. Unfortunately, our homegrown terrorists, many of whom have already returned to our communities having served their sentence or been acquitted on technicalities, are not rehabilitated. They merely walk out of prison, and the onus is back on resource-constrained law enforcement agencies to open a new case and monitor them, ensuring they remain law-abiding citizens. And while in prison, the jihadists have the opportunity to recruit and radicalize others and naturally cross paths with terrorists, gang members, and criminals. By studying the international lessons learned regarding jihadist recidivism, we can effectively cross-apply those tactics, techniques, and observations to our domestic challenges.

Recognizing the growing threat of radicalization of our citizens, US Attorney General Eric H. Holder, Jr., announced the creation of a task force within the Justice Department to combat an "escalating danger" from "homegrown" terrorists within the United States. In his June 4, 2014, announcement, Holder states the task force will chiefly comprise leaders from the FBI, the Justice Department's National Security Division, and US attorneys. Called the Domestic Terrorism Executive Committee (DTEC), it is a re-creation of the task force formed by his predecessor after the 1995 Oklahoma City bombing focused mainly on right-wing domestic terrorists. DETC efforts will be aimed at US citizens or visitors radicalized via the Internet.

JIHADIST DEFINED

According to terrorism expert Dennis Pluchinsky (2008), a jihadist can be defined as a Muslim who believes Islam is under attack by the West

with the objective of destroying Islam, perceives the United States as the primary enemy of Islam, believes it is Islam's manifest destiny to the rule the world, and believes the only proper response to this threat to Islam and the Muslim Ummah (members of the Islamic community) is militant jihad.

Jihadists differ from terrorists who are not religiously motivated. The call to jihad (which means "struggle" in Arabic) is powerful and typically comes in response to a fatwa, or binding religious decree. Jihadists are also revered as martyrs for the cause, which means carefully selecting operational tactics so as not to amplify their deaths. Former Secretary of Defense Donald Rumsfeld once remarked that for every jihadist we kill, we recruit three more (Pluchinsky 2008). Islamic scholar and journalist M. J. Akbar (2002) provides great insight into jihad, describing it thus: "The power of jihad pervades the mind and soul of Islam. The mind is where the current battle will be fought, and this is why it will be a long war."

Recidivism

A recidivist is defined as one who, after release from custody for commission of a crime, is not rehabilitated (Pluchinsky 2008). Although the term is now applied in the counterterror realm, recidivism is closely tracked in the US prison system and the statistics are startling; according to the Department of Justice, an estimated two-thirds (68 percent) of 405,000 prisoners released in thirty states in 2005 were arrested for a new crime within three years of release from prison, and three-quarters (77 percent) were arrested within five years. More than a third (37 percent) of prisoners who were arrested within five years of release were arrested within the first six months after release, with more than half (57 percent) arrested by the end of the first year (Bureau of Justice 2014). Recidivism substantially increased from the previous decade, in spite of extensive education and job training efforts, as well as life skills and readjustment counseling provided to convicts during incarceration. Recidivism by convicted criminals clearly illustrates that arrest, confinement, and rehabilitation alone do not preclude further nefarious activities. The same is true for jihadists, for whom the stakes are much higher.

Counter-Radicalization Efforts

Jihad is a powerful call, and dislodging (or neutralizing) the radical ideology is not an easy task, not even for lifelong Muslims. Many countries have established jihadist rehabilitation and engagement programs, including Algeria, Egypt, Jordan, Singapore, Indonesia, and Malaysia. Notably,

Yemen's program is now defunct and there is no curriculum or facility in place today to process returning Yemeni nationals from Guantanamo.

When releasing detainees from the Guantanamo facility, the US government has heavily relied on the "Saudi program." The program was established after the 2003 bombings in Riyadh and is a "soft" counterterrorism program, meant to combat violent extremism and mitigate the ideological and intellectual justifications of jihad. The program is not punitive, but rather a benevolent, second-chance program with a large social welfare component. Although the exact numbers are questionable, the Saudis claim an overall 80 to 90 percent success rate for the program. They have processed approximately 3,000 individuals and 1,400 have reportedly renounced their former ways and been released. Of the group, there are thirty-five acknowledged recidivists. The rest of the extremists will remain in the program until deemed ready for release. Of 120 Saudi citizens sent to the rehabilitation program from the Guantanamo facility, ten remain in the program and six have been rearrested by officials. Of the 110 released, many reradicalized and became "most wanted" men in Saudi Arabia (Kohlmann 2009).

Inside the Saudi Program

Christopher Boucek is a Middle East specialist who has studied the Saudi approach to recidivism since its inception. His 2008 paper, entitled "Saudi Arabia's 'Soft' Counterterrorism Strategy: Prevention, Rehabilitation, and Aftercare," gives an inside look at this secretive program.

The Saudi program relies on several primary tenets:

- Violent radical Islamic extremism cannot be defeated by traditional security means alone.
- Violent ideology is based on corrupted and deviant interpretations of Islam.
- Obedience and loyalty to the state and its leadership are key.
- Extremists lack the authority and understanding of religious doctrine.

These principles are enforced through a program of co-optation and persuasion by a system called PRAC, which consists of three interconnected phases:

- Prevention: The phase fosters cooperation between the state and the public, highlights the damage done by terrorism and extremism, and ends public support and tolerance for extremist beliefs. Hundreds of programs are aimed at youth in and

out of school; there are also massive public information campaigns, and highway billboards decrying terrorism as part of this phase.
- Rehabilitation: The focal point of this phase is counseling by clerics and academics to reeducate and rehabilitate jihadists. It begins with the assumption that these individuals were misled by extremists who follow a corrupted form of Islam and misinterpret the Koran.
- Post release care: Most Guantanamo returnees entered the program at this point, since they were not tried and convicted of crimes in Saudi Arabia. During this phase, residents live in a "halfway house," the Care Rehabilitation Center. The center has guards and fences, but the prisoners are not confined or restrained in any way. The post release phase focuses on reintegration into Saudi society; the Guantanamo returnees receive additional psychological counseling and participate in activities designed to help them adjust to freedom.

Once an individual has satisfactorily renounced his or her extremist beliefs, job placement services are provided along with other benefits, including a government stipend, a car, and an apartment. The added social support is intended to deter the rehabilitated terrorist from returning to his or her former lifestyle. The Saudi program has been the source of scrutiny; after several former Guantanamo detainees returned to al-Qaeda, DHS sent a team of FBI officials and terrorism specialists to the center for a firsthand look. Although a formal report to the public was not released, one of the team members spoke to the press about his experience. Dr. John Horgan, director of the International Center for the Study of Terrorism at Pennsylvania State University stated, "…when I asked Saudi officers how they knew these people were safe to release, all they could say was they got a feeling." He also opined that prisoners are not being deradicalized and their fundamental views have not changed. Another criticism was the lack of any reliable risk assessment to decide whether an individual should be allowed back into society. "Sex offenders have to meet all sorts of criteria before they are released," Dr. Horgan said. "Why shouldn't it be the same for terrorists?" (Lamb 2010).

Possible Solutions in the United States

In addition to using portions of "PRAC" domestically, a potential model for a domestic rehabilitation program comes from the US military, which successfully delved into the rehabilitation realm in Iraq through the decommissioned Task Force 134 and its "House of Wisdom" program. Through this operation, vetted Iraqi clerics encouraged debate with detainees for the purpose of refuting and mitigating extremist arguments

(Azarva 2009). Also, scientific study shows disengagement of radical ideology is best done through support of an individual's social network (Boucek 2009); therefore, including the American public in the dialogue is a necessity. Avoiding the issue and simply sending the terrorist back to society and our neighborhoods without a support structure is unwise. Finally, the government previously announced intentions to acquire the Thomson Correctional Center, a large, vacant state prison in northwestern Illinois, to house detainees transferred from the Guantanamo facility. Because this plan never came to fruition, perhaps the facility could be used to rehabilitate American jihadists before returning them to society.

We desperately need more comprehensive research and analysis on the issue of recidivism. When contacted for comment regarding his magazine article, Mr. Pluchinsky offered his current view of the situation:

> Jihadist recidivism remains a problem that has not been properly mapped. We have no idea how many released global jihadists turned into recidivists. We still do not know the level and scope of the problem. Most of the evidence, including my 2008 article on the issue in *Studies in Conflict and Terrorism*, is anecdotal. For that matter, terrorist recidivism in general has not been properly and adequately researched.

Very little has been published on the subject in the intervening years, yet global and domestic jihadist activity continues to grow in scope and intensity.

Counterterrorism and homeland security experts are perhaps not the best researchers for this complex issue. Similarly to the analysis of the other terrorism-related issues, the answer may instead lie in the "soft" sciences: psychology, sociology, organizational theory, and theology—disciplines that provide a multifaceted understanding and approach to the problem. Professionals in these fields could best answer the following questions:

- Do religious terrorists have a higher recidivism rate than terrorists without the radical religious ideology? If so, why? What are the implications in the United States?
- Can any parallels be drawn between terrorist rehabilitation and cult deprogramming or the successful neo-Nazi and leftist guerilla rehabilitation programs?
- How can we better use Psy Ops and the Internet to introduce a deliberate theological counterideology to jihad and prevent reradicalization?
- Are there any aspects of the Saudi program that can be applied to would-be domestic terrorists in the United States if they eventually return from detention to our communities?

Recidivism is just one source of manpower for al-Qaeda and other radical Islamic groups seeking to harm the United States and its allies. The ability to tap a US citizen for a mission in his or her home country is something al-Qaeda continues to pursue. Understanding how the switch is flipped from "off" to "on" is critical for prevention, and knowing how to turn it "off" again is fundamental to the domestic deradicalization process. Recidivism is undesirable, but likely unavoidable. There is no such thing as a perfect criminal justice system: The question must be in which direction we want to deflect the likelihood of error.

THE LONE WOLF

According to the FBI, a lone wolf draws ideological inspiration from formal terrorist organizations, but operates on the fringe. Despite their ad hoc nature and generally limited resources, lone wolves can mount high-profile, extremely destructive attacks, and their operational planning is often difficult to detect (FBI 2014). The FBI considers the lone wolf the most significant domestic terrorism threat, especially because detection and mitigation are hampered by relative anonymity. A lone wolf does not necessarily mean one person working alone; Timothy McVeigh's bombing of the Murrah Federal Building in Oklahoma City is a good example. McVeigh and his accomplice were influenced by the ideology of a group, yet they worked clandestinely on the fringe to develop an undetectable plan for mass destruction. Other notable lone wolves include Ted Kaczynski, Eric Robert Rudolph, the perpetrator of the Tylenol poisoning event in 1981, the mailer of anthrax letters just after 9/11, and Joseph Stack, who flew his aircraft into the IRS building. Many of the domestic terror attacks and plots since 9/11 were planned by a lone individual.

Other countries have also experienced horrific lone wolf events against soft targets. Anders Behring Breivik, 32, was a Norwegian lone wolf who planned his operation for nine years and committed two stunning attacks on July 22, 2011. First, Breivik detonated a vehicle-borne improvised explosive device (VBIED) in Oslo outside the prime minister's office, killing eight people. The device was constructed with fertilizer and explosive primer. Breivik then traveled to Utøya Island by boat, infiltrating a Norwegian Labor Party camp for children. Dressed as a police officer to garner unimpeded access and trust from children, he opened fire, killing sixty-nine children and counselors before law enforcement arrived. Breivik surrendered without a fight. With a right-wing extremist ideology and racist, anti-Muslim viewpoints, Breivik believed killing the children was justified. In his estimation, he eliminated the next generation of Marxists who were going to turn Europe into what he calls "Eurabia." Convicted in August 2012, Breivik received the maximum sentence given

IN FOCUS: HUMINT AND DOMESTIC TERROR

Recent domestic cases involving terrorists were foiled not with high-tech equipment, but human sources. Officials in Israel have spoken openly about recent success hindering suicide bombings that had previously caused their country incalculable psychological and economic damage. Although the United States has been spared this particularly brutal means of terrorizing the populace, law enforcement must be ever vigilant of the threat of soft target suicide bombings in public areas such as shopping malls, amusement parks, sports venues, restaurants, and hotels. Lessons learned by Israel and other countries combating suicide bombings are certainly applicable and worthy of analysis by all engaged in the war on terror.

Israel places a high value on human intelligence (HUMINT) and weaves HUMINT into all aspects of its law enforcement activities. A prevalent saying in the country's intelligence community guides its efforts: "The small brings in the big." Israeli law enforcement and intelligence collection agents build long-term, lasting relationships on the ground with all types of business people. For instance, waitresses, bartenders, taxi drivers, and barbers can be a wealth of information. Emergency room employees, gas station workers, and grocery or drug store employees are all good collection sources. Around a specific target, street vendors are worthy of engagement because they frequent the same area and have a perfect viewpoint for noticing out-of-the-ordinary activity. If protecting a church is the objective, the clergy and worshippers are valuable informants. The key is to cultivate the relationship: Visit the sources regularly, build their trust, instruct them on what to look for, and make sure they have a way of contacting you at any time if they notice something suspicious.

Sources are force multipliers and critical to gleaning the information needed to identify, monitor, and then disrupt terrorist activities. As the recent domestic cases illustrate, source cultivation is time well spent by law enforcement. Recent "see something, say something" campaigns will only be effective if we also educate the community on the threat so its members are looking for the right indicators and reporting the most effective details.

in Norway to convicted killers: twenty-one years; after he serves that sentence, his release will be considered by the courts. Breivik published his manifesto on the Internet just prior to executing the attacks, a long missive entitled *2083: A European Declaration of Independence,* and he also posted a video urging conservatives to "embrace martyrdom" and showing himself dressed in a uniform and pointing a Ruger Mini-14 (Berwick/Breivik 2011). A self-professed Freemason and Knight Templar officer, Breivik continues to espouse his right-wing ideology and has started the "Conservative Revolutionary Movement" of activists across Europe from his prison cell. Profiling Breivik would be helpful to understanding the motivation and activities of lone wolves against soft targets, particularly vulnerable citizens such as children.

As these cases amply illustrate, the human behavior and motivations of a lone wolf are broad, complex, and somewhat unpredictable; in this case, the criminal may not be completely motivated by ideology, and many psychological factors, such as anger and paranoia, can be at play. Certainly the radicalized homegrown lone wolf is the most dangerous, fueled by religious ideology and a duty to answer a divine call.

MEXICAN CARTELS CROSS THE BORDER

Just south of our border, Mexican forces are fighting an insurgency against multiple drug trafficking organizations (DTOs) that threaten their country's economy and security. In 2009, the previous director of the CIA, General Michael Hayden, surprised many when he stated: "Escalating violence along the US–Mexico border will pose the second greatest threat to US security this year, second only to al-Qaeda" (Hayden 2009). Furthermore, according to the Justice Department (2011b), Mexican DTOs represent the greatest organized crime threat to the United States. Our government has responded in part by placing thousands of National Guard troops on the border as part of "Operation Jump Start," assisting US Customs and Border Protection. Also, hundreds of federal agents have been pulled from other duties and sent to robust DEA (Drug Enforcement Administration), ATF (Alcohol, Tobacco, and Firearms), and FBI offices in major cities in border states. And despite economic woes, the United States is aiding Mexico's fight against the DTOs under the provisions of the Merida Initiative, a multiyear $1.5 billion antinarcotics package increasing law enforcement cooperation and intelligence sharing between our countries, and supplying training and equipment to the fight. Finally, the $6 billion "virtual fence" project, SBInet, and deployment of expensive aerial drones to monitor the border certainly indicate the government's concern regarding border issues.

Several leaders of the major Mexican DTOs have been indicted on charges within the United States and are fugitives with $5 million rewards offered for capture. This is the same amount offered for the apprehension of "most wanted" terrorists, indicating the serious nature of the threat against our citizens and communities. The players, tactics, alliances, and leaders of the DTOs morph, but the threat to our country persists…and is growing.

Ideology: Money

It is important to understand that, prior to US engagement in the so-called "drug war" beginning in the 1980s, the primary drug trafficking route into the United States was from Colombia, through the Caribbean and into Florida. As we closed off these avenues, but failed to lower user demand in our country, Mexico became the primary conduit for the drug pipeline. As criminal elements exacted their "fee" for moving the product through the country, we witnessed the rise of alliances, or cartels. In addition to moving Colombian drugs, cartels now oversee the cultivation of marijuana and large labs producing methamphetamines. The money at stake is exorbitant; a Justice Department report estimates Mexican and Colombian DTOs generate, remove, and launder between $18 and $39 billion in wholesale drug proceeds annually.

Consider this important fact, which serves to frame the discussion of drugs and the existing or potential nexus with other nefarious groups: Dealers and users in the United States do not care who supplies their drugs. It could be a cartel or al-Qaeda; all that matters is the product and getting it into the hands of the 35 million users in our country, most of whom will give their last dollar or possession to get high. Cocaine is the leading drug threat in the United States, followed by methamphetamine, marijuana, heroin, pharmaceutical drugs, and MDMA (ecstasy). The DTOs have responded to the demand and, with crackdowns at the border, they have moved inside the United States and now oversee the planting of marijuana fields in US national parks. Although surprising, the National Park Service (NPS) reports marijuana has been grown on our public lands for over 25 years. Furthermore, in 2010 and 2011, its internal reports documented the vast amount of marijuana eradicated on NPS land during the period. Between standing plants, or plants harvested and packaged for distribution at the time of interdiction, the NPS estimated a total street value of over $405 million. Nearly all these cases of marijuana grown in national parks were identified as transnational organized crime related operations (Martin 2012).

Tactic: Brutal Violence Against Soft Targets

Protecting this vast drug enterprise is critical for the DTOs. In Mexico, the areas of operation for the cartels are called *plazas*. Pipelines are the supply corridors into, through, and out of Mexico, safely passing through the plazas in which the cartels have the upper hand by bribing or intimidating officials and citizens. Some of these formerly vibrant areas have turned into ghost towns due to the persistent escalating violence unleashed by the DTOs to maintain control of the *plazas,* most of which are at the US/Mexico border.

DTO violence is like none before. The perpetrators have no respect for the rule of law and employ no moral restraint, willfully (and exuberantly) killing innocent people every day. Kidnapping, rape, human trafficking, extortion, larceny, arson, and weapons offenses—nothing is off the table for DTOs in the name of making money, widening their sphere of influence, and controlling plazas and pipelines. DTOs are transnational organizations; the US National Drug Intelligence Center reports that not only are they operating in the United States and nineteen Latin American countries, but they are also present in unexpected regions, such as Australia. This indicates their global reach and ability to transport their products worldwide.

Prior to December 2006, DTO violence was sporadic and contained by the government. During the election that year, Mexican president Felipe de Jesús Calderón Hinojosa stated that his primary goals were to grow his country's economy by creating jobs and reducing poverty. However, once in office in late 2006, President Calderon opened a strategic front against the DTOs, declaring "war" against the cartels. Interestingly, this action was not unilaterally supported by the citizens of the country, whose small towns benefit financially from the movement of drugs through the area. Also, as they feared, innocent civilians inadvertently ended up on the frontlines of the battle. At least 130,000 people were killed in the violence between the start of President Calderon's offensive and June 2014, or about two every hour. These numbers do not include the 27,000 kidnapped and missing citizens, suspected to have suffered brutal deaths at the hands of the cartels, with their bodies unceremoniously dumped in the desert (Molloy 2013).

The battle between cartels for control has led to the preponderance of these mainly civilian deaths. The cartels target the government, with bombs regularly exploding in front of police stations and at city halls. However, soft target attacks have been a more compelling way for cartels to push their agendas. Shootouts in the street happen daily, as thousands of videos taken by civilians and posted on the Internet attest.

Innocent men, women, and children caught in the crossfire are seen by DTOs as collateral damage and are now the very targets of the rampant violence by groups sending "messages" to towns and each other. Many murders, such as beheadings, death by gasoline-induced fire, dismemberment, and acid baths, are premeditated and gruesome. Politicians and policemen are often hung in effigy from bridges in major cities with signs threatening those who are battling the cartels to back off. In January 2010, thirty-six-year-old Hugo Hernandez was kidnapped in the state of Sonora by Sinaloa cartel members, who carved his body into seven pieces, dropping them at separate locations. Finally, his face was sliced off and stitched to a football, which was delivered to city hall with a warning to the Juárez cartel (Rodriguez 2010). Cartel violence often begets violence; a few days later, masked gunmen attacked teenagers in the border city of Ciudad Juárez—children who were enjoying a combination birthday and high school soccer victory party—leaving sixteen dead and fourteen wounded. The very same evening in Torreon, in the border state of Coahuila, gunmen ambushed students in a college bar: ten were left dead and eleven wounded. In the case of the children and college student massacres, the shootings were simply meant to send a message to rival cartels, law enforcement, and government leadership, with a by-product of terrorizing the public (Jasper 2010).

Many of these activities are carried out by the "enforcement arms" of the cartels, which are paramilitary groups possessing the training, knowledge, and sophisticated equipment of small armies. Street gang spinoffs of the main organization will also accomplish some of this dirty work, so if they are apprehended by authorities, the main leadership of the cartel and its business activity remain unaffected.

Goals: Money, Power, Control

The primary goal of cartels is to gain power, territory, and control so they can move drugs, money, guns, and human cargo unopposed. They seek to create a void in leadership and rule of law in cities so that they can step in and take control. Corruption of police, military, and government leadership is a tool used to create instability, ruin the government's reputation with citizens, and cause citizens to turn to others for protection. Instilling fear in the populace is a primary goal, compelling citizens to assist the DTOs or, at the very least, not resist their land grabs and activity in the community. Anything and anyone standing in the way of the cartels' progress is seen as a threat that must be eliminated. Conversely, anything and anyone helping attain their goals is an ally.

MAJOR DTOS IMPACTING THE UNITED STATES

For an in-depth look at the individual cartels, please see my previous work in Chapter 5 in *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups* (Hesterman 2013) For purposes of the discussion regarding soft targets, it is important to know that all of the major DTOs now have a presence in the United States.

According to a report by General McCaffrey and Dr. Robert Scales (2011), "Drug cartels exploit porous borders using all the traditional elements of a military force, including command and control, logistics, intelligence, information operations and the application of increasingly deadly firepower." Indeed, the DTOs have slipped past the border and into our heartland, and nearly every state in our country is experiencing Mexican DTO activity. The cartels are using multiple points of entry at the border via plazas or tunnels, leveraging contact with gangs inside the United States to move drugs, and recruiting. In 2008, DTOs were present in 230 cities in the United States; startlingly, this number rose to more than a thousand US cities by 2010, according to the US Justice Department's National Drug Threat Assessment (2011b).

Cartel violence is emerging in our cities, especially in border states such as Arizona. As violent crime rates in the nation continue to fall dramatically, they are increasing in Arizona across the board. Phoenix has not enjoyed the same decrease in murders as other cities, such as New York City, which saw a 20 percent decline in homicides in 2013. The state is also starting to experience the cartel's brand of brutal violence. The first beheading by a DTO in the United States occurred in an apartment in Phoenix in 2010, carried out by a member of the Sinaloa cartel (Associated Press 2013). DTO-related home invasions in the Phoenix area are also on the rise; in June 2008, several men wearing Phoenix Police Department uniforms forced their way into a Phoenix home, killing an occupant and spraying the home with fifty to one hundred bullets. In addition to violent home invasions, kidnappings in Phoenix are also prevalent; in fact, Phoenix is now the number two kidnapping capital of the world, behind Mexico City. DTOs, especially the Zetas, use kidnappings to obtain demands; however, even if demands are met, the kidnapping typically ends in murder.

The cartels routinely issue a "green light," authorizing the killing of police and military. According to the Department of Homeland Security, in 2010 the Barrio Azteca issued a green light authorizing the murder of law enforcement officers in El Paso (DHS 2010). The Barrio Azteca gang formed in Texas prisons in the 1980s and is affiliated with a Mexican gang, the Aztecas, who carry out hits for the Juárez cartel's

La Linea enforcers. Shortly after the green light was given, the Aztecas targeted and killed pregnant US consulate employee Leslie Ann Enriquez Catton and her husband at the border in Ciudad Juárez. The husband of another consulate employee, Jorge Salcido, was also killed in the attack. Miraculously, the Catton's young child, strapped in a car seat, was unharmed (US Department of Justice 2010). High-profile murders of US law enforcement agents by DTOs include ICE Special Agent Jaime Zapata and Border Patrol Agent Brian Terry.

Special Concern: Los Zetas

Imagine, for a moment, that one of America's elite special operations units goes "rogue" and starts using its specialized skills, equipment, and training *against* the US government. The members of the unit participate in illegal activities such as drug trafficking, gun running, and human smuggling. They also serve as hit squads, willing to murder innocent victims in return for cash. The unit does not fear, hide, or run from law enforcement; rather, it engages.

Meet the Los Zetas organization. The fastest growing DTO in Mexico, this is the first to use the Internet, the first to savagely behead innocent civilians to send "warnings," and the first to drop propaganda leaflets from aircraft. With an estimated membership of two thousand, the core of the Zetas is composed of former members of the Grupo Aeromóvil de Fuerzas Especiales, or the GAFE. The GAFE is the Special Forces arm of the Mexican army; its members receive specialized training in jungle, amphibious, urban, and high-mountain operations from the best counterterrorism and counterinsurgency units in the world. They are also trained to deploy forward into hostile foreign territory and to blend in and operate undetected. In recent years, the GAFE's primary mission morphed from providing protection to key officials and buildings to one of assisting the country in dismantling drug cartels. Along with their counterintelligence, disguise, and insurgency training, the Zetas are a complex and lethal force. Although other paramilitary or "enforcement groups" are present in every cartel, such as the CJNG (Knights Templar), the DEA labels the Zetas as "the most technologically advanced, sophisticated, and violent" (DEA 2008).

Zetas Tactics

Zetas should not be viewed as a criminal enterprise, but as a lethal, complex army. They have specialized training in navigating and operating in

all terrains; they have river swimmers, divers, jungle experts, and training in urban warfare. Money from their drug trade and other nefarious activity enables Zetas to buy top-of-the line equipment; they have tanks, surface-to-air missiles, rocket-propelled grenades (RPGs), night-vision equipment, boats, helicopters, and aircraft. They often operate in small fire teams and use snipers and countersnipers.

Their executions are savage; they often set their targets on fire, decapitate them, or saturate their bodies with bullets. The scope of violence is escalating; in May 2012, Lazcano gave orders for the massacre and dismemberment of forty-nine innocent civilians in the so-called "Mother's Day Massacre." They also engage law enforcement and the military, using ambush tactics and the element of surprise to kill officers before they can react.

We should not underestimate the sophistication of the Zetas; undetected, they plan and practice for operations, performing surveillance and patiently waiting for the right time to strike. The brazen daytime attack on a casino in Monterrey, Mexico, in August 2011, which left at least fifty-two people dead, is an example of the escalation and calculation of Zeta violence. Twelve gunmen entered the casino and started shooting into the crowd; other attackers simultaneously doused exits with gasoline and threw grenades into the building to start multiple fires. Such attacks are less about the target (in this case, a casino) and more about the message. Clearly, the Zetas are not merely a criminal element; they use terroristic tactics to further their goals.

The Zetas are also known for their *sicarios,* or assassins. Take the case of Rosalio Reta, a US citizen born and raised in Laredo, Texas. At 13 years of age, Reta was kidnapped by Zeta members and taken to Mexico, where he became a Zetita, or "little Zeta," attending tactical training camps. His initiation came shortly thereafter, when he was directed to shoot a man in the head at a bar in Nuevo Laredo. He returned to live in Laredo at the age of 15, where he was used by the Zetas to kill several men and young boys throughout Texas. Reta's assassinations and apprehension are detailed in the 2012 book, *The Executioner's Men,* by George W. Grayson and Samuel Logan, the most comprehensive book available on the Zetas.

Increasing Reach in the United States

In addition to *sicarios,* the Zetas have clearly been operating in the border region for many years; however, the stunning 2011 arrest of fifteen Zetas in Chicago perfectly illustrated the reach of the group within our borders. The case detailed the movement of drugs from Nuevo Laredo,

Mexico, through Texas and into Chicago, via a US fugitive working for the Zetas. The street value of this cell was staggering: Feds seized 12 million US dollars in cash and 250 kilograms of cocaine (DEA 2012). According to the FBI, in addition to all of the border states, Zeta cells are believed to be present in Tennessee, Oklahoma, South Carolina, and Georgia (FBI 2008).

A battle is also raging for control of Interstate 35, a highly desired route for drug traffickers. I-35 begins at the border in Laredo and traverses major cities like Dallas, where, according to a Justice Department memo, Zetas have been active since 2003 as part of the Gulf cartel. Following the shooting death of Dallas Police Officer Mark Nix, law enforcement agents have been looking for Maximo Garcia Carrillo, a suspected Zeta and the triggerman in the shooting who owned a house in the Oak Cliff suburb of the city. On the other side of Dallas, I-35 has intermittent empty stretches of highway, but eventually passes through Oklahoma City, Kansas City, and Minneapolis. The interstate ends in Duluth, Minnesota, at the Canadian border. The importance of this corridor to the cartels is significant; as the former head of the DEA's El Paso Intelligence Center once stated, "Drug traffickers kill for I-35." More recently, the Zetas have also become involved in the human smuggling business, charging a 10 percent commission for use of their border plazas, pipelines, and the Interstate 35 corridor. It seems incredible that Zetas charge smugglers to operate on US real estate, and it is even more egregious that they would buy property and live illegally in our cities, right under the nose of law enforcement (Hesterman 2009).

Nexus with Gangs

The Zetas are increasingly wielding control over US gangs such as MS-13, the Mexican Mafia, and the Texas Syndicate. The FBI's gang assessment indicates a number of alarming trends, including that street gangs in the United States are growing in size, operating at the border, and forming ties with DTOs (US Department of Justice 2011c). The imitation of tactics typically indicates some type of liaison at the training or operational levels; gang members in our country are now engaging in nontraditional crimes such as human trafficking and alien smuggling. They are acquiring high-powered weaponry and showing new sophistication in terms of recruitment and communication. These attributes make them attractive to cartels to work their street-level issues, launder money, and move product. Law enforcement believes the Zetas may have already used MS-13 in several operations in the United States, providing training and weaponry.

Domestic Terror Group	History/Propensity for Hitting Soft Targets?	With Intent to Kill?	Reach?	Capability?
Right Wing Religious	Yes	Likely	Yes	Yes
Right Wing Militia	Possibly	Possibly	Maybe	Maybe
Right Wing Sovereign	Yes	Yes	Yes	Maybe
Left Wing Anarchist	Yes	Unlikely	Yes	Maybe
Left Wing Single Interest (Animal, Eco, etc.)	Yes	Unlikely	Yes	Maybe
Homegrown Jihadist	Yes	Yes	Yes	Likely, training outside the U.S. or through online propaganda
Lone Wolf of any ideology	Yes	Yes	Yes	Maybe
Drug Trafficking Organizations (Cartels)	Yes	Yes	Yes	Maybe, through street gangs

FIGURE 4.2 Summary of domestic threats against soft targets.

SUMMARY OF DOMESTIC TERRORIST THREATS AGAINST SOFT TARGETS

As the chapter illustrated, the domestic terror threat is vast and growing (Figure 4.2). Many groups have already targeted innocent civilians to further their political or religious goals and have a propensity, reach, and/or capability to hit soft targets in the United States.

Now that we understand the vast international and domestic threats to our country and its citizens, we next take an in-depth look at their potential targets and our vulnerabilities.

REFERENCES

Akbar, M. J. *The Shade of Swords: Jihad and the Conflict between Islam and Christianity.* London: Routledge, 2002.

Associated Press. "Crisantos Moroyoqui-Yocupicio Gets 14 Years in Cartel Beheading in Arizona" (May 8, 2013).

Azarva, Jeffrey. "Is U.S. Detention Policy in Iraq Working?" *Middle East Quarterly* Winter 2009 (2009): 5–14.

Bergen, Peter and Bruce Hoffman. "Assessing the Terrorist Threat." September 10, 2010. http://bipartisanpolicy.org/sites/default/files/NSPG%20Final%20Threat%20Assessment.pdf

Boucek, Christopher. "Clearing a Path for Guantanamo Returnees: Rehabilitation and Risk-Assessment." Carnegie Endowment for International Peace. http://www.carnegieendowment.org/2009/01/28/clearing-path-for-guantanamo-returnees-rehabilitation-and-risk-assessment/34l (2009).

———. "Saudi Arabia's 'Soft' Counterterrorism Strategy: Prevention, Rehabilitation, and Aftercare." In *Carnegie Papers,* 2008.

Breivik, Anders Behring. "2083—A European Declaration of Independence." http://www.youtube.com/watch?v=KjCy90NVLQM

(Breivik), Andrew Berwick. Anders Behring. "2083: A European Declaration of Independence" (2011).

Bureau of Justice. "Recidivism of State Prisoners Released in 2005." 2014.

Burke, Jill. "Guide to Alaska Sovereign Citizens Trial: Patriots, Militias and Going to Extremes." http://www.alaskadispatch.com/content/guide-alaska-sovereign-citizens-trial-patriots-militias-and-going-extremes (May 20, 2012).

Bynum, Russ. "Prosecutor: Army Soldiers Planned Terror Plot." *Northwest Herald* (2012). http://www.nwherald.com/2012/08/27/prosecutor-army-soldiers-planned-terror-plot/a9cmznn/.

"C4ss: Center for a Stateless Society." http://c4ss.org

CBS News. "Man Angry at IRS Crashes Plane into Office," February 19, 2010.

Cecil-Cockwell, Malcolm. "The Earth Liberation Front: Sabotaging a Way of Life." *Epoch Journal* 2, no. 3 (2008).

Cohen, J. Richard. "Why It's Time to Take Domestic Terrorism Seriously" (2014).

DEA (Drug Enforcement Administration). "National Drug Assessment" (2008).

———. "Twenty Charged in Chicago with Various Drug Trafficking Offenses, Including Five Allegedly Tied to the Mexican 'Zetas' Cartel" (2012).

DHS. (Department of Homeland Security). "Officer Safety Alert" (2010).

———. "Right Wing Extremism" (April 7, 2009).

FBI (Federal Bureau of Investigation). "Los Zetas Expanding Reach into Southeast and Midwest United States" (2008).

———. "Sovereign Citizens: A Growing Domestic Threat to Law Enforcement." Counterterrorism Analysis Section, http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/september-2011/sovereign-citizens (2011).

———. "FBI Strategic Plan 2004–2009."

Galofaro, Claire. "7 Suspects in St. John Deputy Shootings Are Tied to Violent Anti-Government Group." http://www.nola.com/crime/index.ssf/2012/08/7_suspects_in_st_john_deputy_s.html (August 17, 2012).

Gartenstein-Ross, Daveed and Madeleine Gruen. "Leadership vs. Leaderless Resistance: The Militant White Separatist Movement's Operating Model." *Foundation for Defense of Democracies* http://www.defenddemocracy.org/media-hit/leadership-vs-leaderless-resistance-the-militant-white-separatist-movement/ (February 18, 2010).

Grayson, George W., and Samuel Logan. *The Executioner's Men: Los Zetas, Rogue Soldiers, Criminal Entrepreneurs, and the Shadow State They Created*. New Brunswick: Transaction Publishers, 2012.

Hayden, Michael, Armed Services Committee, Confirmation Hearing, May 12, 2009.

Hesterman, Jennifer. "The Mexican Drug War Spills over the Border." *The Counter Terrorist* (2009): 26–38.

———. "Catch and Release: Jihadist Recidivism." *The Counter Terrorist Magazine* (April/May 2010).

———. *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups*. Boca Raton, FL: CRC Press, 2013

Hoffman, Bruce. "Sources of Concern and Future Prospects." In *Recent Trends and Future Prospects of Terrorism in the United States*: RAND Corporation, 1988.

———. *Inside Terrorism*. New York: Columbia University Press, 2006.

Jasper, William F. "Escalating Chaos on Our Border." *The New American* (2010): 17.

Kohlmann, Evan F. "'The Eleven': Saudi Guantanamo veterans Returning to the Fight." http://counterterrorismblog.org/2009/02/nefa_report_-_the_eleven_saudi.php

Lamb, Christina. "Guantanamo Closure Delayed Amid Rehab Failures." *The Australian News* (2010). Published electronically January 11, 2010. http://www.theaustralian.com.au/news/world/guantanamo-closure-delayed-amid-rehab-failures/story-e6frg6so-1225817851821

Martin, Robert R. "The National Park Service and Transnational Criminal Organizations—Is a Crisis Looming?" American Military University, 2012.

McCaffrey, Robert H. and Barry R. Scales. "Texas Border Security: A Strategic Military Assessment," Colgan LP, 2011.

McNabb, J. J. "'Sovereign' Citizen Kane." *The Intelligence Report*, no. 139 (2010).

Molloy, Molly. *Small Wars Journal* August 21, 2013.

NAALPO (North American Animal Liberation Press Office). http://animalliberationpressoffice.org/NAALPO/

National Consortium for the Study of Terrorism and Responses to Terrorism. "Understanding Law Enforcement Intelligence Processes," July, 2014. www.start.umd.edu

Olson, Dean. "Agroterrorism: Threats to America's Economy and Food Supply." *FBI Law Enforcement Bulletin (February 2012)*.

Pluchinsky, Dennis A. "Global Jihadist Recidivism: A Red Flag." *Studies in Conflict & Terrorism* 31, no. 3 (2008).

Rodriguez, Olga R. "Mexico Cartel Stitches Rival's Face on Soccer Ball" (2010).

Shelley, Louise I. "Methods and Motives: Exploring Links between Transnational Organized Crime & International Terrorism." US Department of Justice, 2005.

Simcox, Robin and Emily Dyer. *Al-Qaeda in the United States: A Complete Analysis of Terrorism Offenses*. London: Henry Jackson Society, 2013.

Sofer, Ken and Molly Bernstein. "17 Years after Oklahoma City Bombing, Right-Wing Extremism Is Significant Domestic Terror Threat." Think Progress, http://thinkprogress.org/security/2012/04/19/467384/chart-right-wing-extremism-terror-threat-oklahoma-city/?mobile=nc (2012).

"The Solution, Schaeffer Cox Speaks on the Future of the Liberty Movement" (2012).

"Ten Years after 9/11: An Anarchist Evaluation." *Anarchist Developments* 1(2011). http://www.anarchist-developments.org/index.php/adcs/issue/view/5/showToc

US Department of Justice. "35 Members and Associates of Barrio Azteca Gang Charged with Racketeering," news release, March 9, 2011. http://www.justice.gov/opa/pr/2011/March/11-ag-299.html (2011a).

———. "Eleven Defendants Indicted on Domestic Terrorism Charges" (2006).

———. "National Drug Threat Assessment." National Drug Intelligence Center (2011b).

———. "National Gang Threat Assessment" (2011c).

———. "Nine Members of a Militia Group Charged with Seditious Conspiracy and Related Charges," news release, March 29, 2010. http://www.justice.gov/opa/pr/2010/March/10-ag-334.html

Zuckerman, Jessica. "60 Terrorist Plots since 9/11: Continued Lessons in Domestic Counterterrorism." Heritage Foundation, 2014.

CHAPTER 5

Soft Target Threat Assessment
Schools, Churches, and Hospitals

> Kazbek Misikov stared at the bomb hanging above his family. It was a simple device, a plastic bucket packed with explosive paste, nails, and small metal balls. It weighed perhaps eight pounds. The existence of this bomb had become a central focus of his life. If it exploded, Kazbek knew, it would blast shrapnel into the heads of his wife and two sons, and into him as well, killing them all.
>
> **—C. J. Chivers, from "The School" (*New York Times* 2007)**

INTRODUCTION

Kazbek Misikov and his family started September 1, 2004, on a wonderful note; it was the first day of school and he, his wife, and two sons dressed up and went to the Beslan School for the special "Day of Knowledge" welcome-back ceremony that began at 9:00. At 9:20, with 1,200 children, teachers, and staff in the gym, Chechen separatists attacked. The next four days were hell on earth for those who were unable to escape; Mr. Misikov and his family were injured, but fortunately, came out alive. Sadly, 330 innocent people lost their lives in the siege, including 108 children.

Every day, somewhere in the world, a school, church, or hospital is attacked by a terrorist or insurgent group, usually one that has also threatened the United States or its citizens. The psychological vulnerabilities covered earlier are only part of the challenge related to protecting people from these types of heinous soft target attacks. There are also physical vulnerabilities that make soft targets more attractive to would-be attackers—some that can be mitigated, and others that cannot. Prior to discussing individual venues, we start with a strategic view of the United States to assess vulnerability of certain regions and cities and then we explore the targets themselves.

VULNERABILITY IN THE UNITED STATES

If I asked you to name the top four US cities most vulnerable to a terrorist attack, the natural response is those with large populations and symbolic targets such as Washington, DC and New York City. Would it surprise you to know that a government-funded study, conducted by mathematicians and statisticians, produced a wholly different list?

In 2007, a groundbreaking report rated 132 US cities on their vulnerability to terrorist attack using a newly developed statistical method. "Benchmark Analysis for Quantifying Urban Vulnerability to Terrorist Incidents" was written by Dr. Susan Cutter, a hazards and vulnerability expert and Dr. Walter W. Piegorsch, a leading statistician and environmental risk expert (Piegorsch, Cutter, and Hardisty 2007). The study was funded by the Department of Homeland Security and yielded some unanticipated results.

The overarching goal was to analyze the relationship between location vulnerability and terrorist outcome. Taking a new approach, the study calculated the susceptibility of areas to attack by assessing socioeconomic factors and demographics as a way to predict the impact of an attack on the populace, and to assess the likely response of residents. Natural geographic features and environmental hazards were also considered, as well as critical industries, ports, railroads, bridges, tunnels, water/sewage systems, and the age and fragility of the existing infrastructure. Finally, the team analyzed and factored in historical data from the terrorism knowledge base and the global terrorism database. Although most Americans can only recount a handful of terrorist attacks if asked, the research considered over one thousand unique terrorist-related incidents in US cities, spanning a thirty-year period. A surprising result is that, contrary to typical threat assessment criteria, areas with nuclear power plants and military facilities did not come up as "high risk" in the analysis.

The final computation of factors resulted in a place vulnerability index, or PVI, rating. Overall results presented on the chart in Figure 5.1 indicate the eastern and southern seaboards of the United States are at greatest risk and also show a large swath of vulnerability from Texas to Ohio. Cities scoring the highest place vulnerability index (PVI) can be seen in Figure 5.1.

Other major areas typically thought of as vulnerable were much lower in ranking, even falling below Columbia, South Carolina, which had a PVI of 1.117. For example, Los Angeles, California, had a PVI of 0.421; Dallas, Texas, a PVI of 0.447; and Denver, Colorado, a PVI of 0.171. Surprisingly, Seattle, Washington's PVI was very low, at –0.315. To view the map with color code results and more detailed computation information, please access the study (Piegorsch et al. 2007).

City	PVI
New Orleans, LA	3.110
Baton Rouge, LA	3.061
Charleston, SC	2.543
Norfolk, VA	2.326
New York/Newark area	2.154
Washington, DC area	1.978
Houston, TX	1.844
Philadelphia, PA	1.737
Boise, ID	1.696
Atlanta, GA	1.683
Chicago, IL	1.404

FIGURE 5.1 Place vulnerability index (PVI).

SMALL CITIES AND RURAL AREAS IN THE CROSSHAIRS

Cities previously hit or targeted by terrorists have been hardened with hundreds of millions of dollars of taxpayer money. But those few urban areas represent less than 5 percent of the US population; what about everyone else? Not only are the top four cities identified in the study as vulnerable to attack surprising, but Boise, Idaho, with a population of 220,000, emerged as a new area of concern, the lone red "blip" in the northwest. Although funded by the government, the study's results were not widely disseminated to the public or covered by the news media. Boise city officials acknowledged surprise at the results, engaging with both Piegorsch and the state's Homeland Security officials for clarification. In 2008, I blogged about the study's results on the Internet and was contacted by several concerned citizens from Baton Rouge and chided by one for "painting a bull's-eye" on his city. Instead of responding emotionally to studies such as this one, it is more helpful to appreciate how the study illuminates a pathway to greater awareness, inspires businesses and community institutions to review security procedures and review terrorism insurance coverage, and may even be used as a vehicle to lobby the government for target-hardening funding. Therein lies the conundrum: Do citizens truly want to know their vulnerability to terrorist attack? Bad actors hope we become passive bystanders or, worse, remain in blissful denial so they will not have to fight us on the way to the target.

The standard perception in our country is that smaller cities and rural areas are not vulnerable to attack by international or domestic terrorists. For example, the Terrorism Risk Insurance Act (TRIA) was

enacted in 2002 as a response to the 9/11 terrorist attacks as a public–private partnership requiring private insurance companies to provide terrorism risk coverage, with federal funding as a backstop if costs to insurance companies exceed $100 million. The law was renewed in 2005 and 2007 and is set to expire in December 2014. Critics argue that not only does the law place an unnecessary burden on taxpayers, it puts an undue cost on those living in rural areas with "less of a terrorism threat" (Novak 2014). The critics are not looking at vulnerability studies or data from our law enforcement agencies that show rural areas are now being preyed upon and exploited by violent gangs, drug cartels, and organized crime.

For instance, in 2009, the DEA discovered during Operation Xcellerator that the Sinaloa's drug cartel hubs were not in major metropolitan areas as previously thought, but rather the cartel was using unsuspecting rural areas to move product. One distribution center was located in Stow, Ohio, a quiet community of 35,000. The Sinaloas were using the small airport to move drugs between Stow and distribution hubs in California (US Department of Justice 2009). In rural Rhode Island, the La Cosa Nostra (Mafia) allowed the Hells Angels outlaw motorcycle group to continue illegal trafficking activities on their turf without interfering, in return for the bikers paying a percentage to the mob. According to the FBI, the unlikely, dangerous relationship between the Hells Angels and the Mafia continues today (WPRI Newport, Rhode Island, 2008). Who would predict quiet Stow and rural Rhode Island would be host to such violent transnational actors? The presence of organized crime or cartel activities in a rural area is a red flag for an even more vexing threat: terrorists often prey on established routes, and groups with different goals are increasingly working together.

The place vulnerability study teaches us much about risk assessment, and its methodology can be applied in any country to similarly illuminate the gap between perceived and actual vulnerability. The study's surprising results indicate that probability, not vulnerability, is driving the government's security focus and funding streams.

HOW BAD ACTORS CHOOSE TARGETS

Before discussing the soft targets themselves, it is essential to get inside the minds of criminals, especially killers. In 2014, I attended an international security conference in Dubai and was fortunate to meet Dr. Martin Gill, a renowned British professor of criminology and author of several outstanding publications that view crime through the eyes of the criminal (Gill 2014). His field work includes interviews with convicted killers about their crimes, to assess motives and the real versus perceived

usefulness of closed circuit television (CCTV), store security guards, alarm systems, and other physical security apparatus. When posed the question regarding how criminals choose their targets, Dr. Gill's answer is simple: because they are easy. Gill found that CCTV does not affect the way criminals commit their offenses, as they merely wear a disguise or pull a hat down low and look at the ground. They bet the cameras are not working or if they are caught and facing prosecution, the burden will be on the prosecutors to prove it is them in the video. In fact, some criminals have shared that if they believe during the course of the crime that their image has been captured on CCTV, the severity of the crime may escalate. One convicted murderer commented that if he was going to spend a long time in prison anyhow, he might as well kill, saying "They've taken away my incentive *not* to kill." Another stated, "If I'm going to jail for armed robbery and I need to kill someone in order to get away, I may take that next step." In fact, one man in prison for murder said that if it is a risky crime, the decision to shoot and kill a lone security guard is actually easy. It eliminates the one piece of evidence that will always stand in court: visual recognition of the perpetrator. Criminals report being more concerned about being stopped by people than any type of technology. They also note favoring large, bulky security guards because they can be outrun. As shown in this example regarding the potential ineffectiveness of CCTV, seeing the potential crime scene through the eyes of a criminal is invaluable to the discussion of target hardening.

THE SOFT TARGETS

Although successfully hitting a hard target such as a government building, military base, or a symbolic target brings credibility to a terror group, a soft target attack would certainly damage the national psyche and discredit the government's ability to protect its people. Factor in the use of a chemical or biological agent, or radiation, and the impact could be immense on sectors such as tourism, shopping, and recreation.

All citizens have the right to learn, worship, and receive medical care in a safe environment. However, we all can easily slip into a false sense of security in these facilities and become complacent about safety. Security is also not the primary goal of these institutions, which are typically resource constrained and do not have money to spend on extra security measures or guards, adding to their vulnerability. Also, these are typically "gun-free" zones, so the only resistance a bad actor will meet is a security guard or two, typically not armed. This combination of factors makes schools, churches, and hospitals targets of choice for terrorists or homicidal killers.

SCHOOLS

On April 7, 2011, a 24-year-old man named Wellington Oliveira traveled to the Tasso da Silveira Municipal School in Rio de Janeiro where, as a former student, he had been subject to bullying. He methodically killed twelve students. A firefighter who responded to the scene told newspapers "There is blood on the walls, blood on the chairs. I've never seen anything like this. It's like something in the United States" (Johnson 2012). His statement illustrates the prevailing worldview toward the escalation of violence in our country, especially with the recent epidemic of school shootings and stabbings that garner wide press coverage.

Perhaps nothing more deeply affects the American public than an attack at a school. It is never expected that innocent children would be targeted by anyone, be it a fellow student, a member of the community with a mental illness, a criminal, or a terrorist. Therefore, we are wholly unprepared, shocked, and deeply saddened. The ripple effect of school attacks is also immense, traumatizing students, teachers, and first responders who view the scene, inducing posttraumatic stress and panic disorder in many.

At any given time, there are at least 75 million Americans attending some type of school from kindergarten (K) through doctorate level courses, and there are five million teachers, administrative, and support staff on campuses (DHS 2012). Many schools also serve community needs and can be used as places for meeting or polling, or as shelters in times of emergency. Even if schools are not the terrorists' intended target and their act of violence is a city building or mass transit, children must be protected from physical and emotional side effects of being in proximity to such horrific violence. For example, there were four elementary schools and three high schools located within six blocks of the World Trade Center on 9/11, and thousands of children were exposed to the toxic dust clouds from the collapsing buildings. Children in at least three states had parents working in or around the World Trade Center that day; in the Washington, DC, area, schoolchildren faced similar stress when the Pentagon was attacked (CDC 2003).

The top two deadliest mass shootings by a single person in US history both occurred on school campuses. On April 16, 2007, 23-year-old Seung-Hui Cho killed two students in his dormitory and then went to a classroom building, barricaded himself inside, and shot fifty-three students and teachers, killing thirty in just nine minutes. On December 14, 2012, Adam Lanza killed his mother in their home and then went to the Sandy Hook Elementary School in Newtown, Connecticut. There, he bypassed the security door and shot through a plate glass window to gain entrance to the building. He killed twenty first-graders and six staff members in only six minutes. Since the 1999 Columbine attack by students Eric Harris and Dylan Klebold, which killed fifteen students and

injured twenty-four, there have been thirty other major school shootings in our country. The terrorists are watching and see the relative ease with which these school attacks are accomplished.

Gun attacks are obviously the most feared assault, because mass casualties can be inflicted in a short period of time. However, more knives than guns are confiscated in schools across the country annually, and knifing incidents are increasing in the United States. Between April 2013 and April 2014, there were at least ten reported stabbings at schools across the country. Knife attacks are fast, unexpected, and devastating in terms of injuries. For example, on April 9, 2013, fourteen people were injured in a stabbing attack at the Lone Star College in Texas. Dylan Quick, a 20-year-old student, used an X-ACTO knife and a scalpel, purposely stabbing victims in the head. The fast-paced attack ended when the suspect was subdued by students. On April 9, 2014, sixteen-year-old Alex Hribal used two kitchen knives to stab twenty-two victims in their stomachs and lower backs at Franklin Regional High School outside Pittsburgh, Pennsylvania. The devastating attack took less than five minutes and Hribal, too, was subdued by fellow students. Thankfully, no one was killed in his rage attack. In stabbings, victims often do not realize what has happened until they start bleeding, delaying the "fight or flight" response and allowing the attacker more time to engage and to inflict wounds. Reviewing case studies, it appears people may be more willing to engage and subdue an attacker with a knife, choosing to run or hide from a gunman. However, engaging an enraged assailant who is wielding large knives is very difficult, and those who approach are likely to be injured. The United States is not the only country faced with this issue; mass stabbing attacks have also occurred in primary schools around the world, with mass casualty attacks in Ireland, China, and Germany.

The kindergarten through twelfth grade vulnerability differs from that on a college campus. First of all, a younger populace cannot defend themselves as readily and are more likely to slip into suspended disbelief as the situation unfolds instead of experience a flight or fight response. College campuses have their own vulnerabilities related to the culture of openness, physical location in the community, poor partnering with or distrust of external law enforcement, and nefarious elements to which they are already exposed such as drugs and even espionage. Examining the unique vulnerabilities associated with K–12 and colleges and universities helps to understand trends, the risk of attack, and mitigation challenges better.

K–12 in the Crosshairs

The first K–12 school attack in the United States was the Enoch Brown School massacre, which occurred July 26, 1764. On this date, four

American Indian warriors entered a white settler's log cabin school in Greencastle, Pennsylvania, and used a tomahawk to kill and scalp the teacher and ten students. Throughout the years, primary and secondary schools have been the sites of revenge murders, racial attacks, gang violence, suicides, workplace violence, and lover's quarrels. They have also been used by domestic terrorists as a way to express rage and garner attention to their cause. For example, on May 18, 1927, the Bath Consolidated School was the scene of the deadliest act of mass murder in a school in US history, a lone-wolf, antigovernment attack. Andrew Kehoe, upset with policies and tax law he believed led to his farm foreclosure, murdered his wife at home and then detonated three dynamite bombs at the Maine school, where he worked as the accountant (Figure 5.2). Kehoe spent months planting explosive material throughout the building in a premeditated act that stunned the country. When confronted at the scene by law enforcement, he detonated a vehicle bomb, killing himself and the school superintendent. In all, the attack killed thirty-eight school children and five adults.

Modern-day schools have been used as political targets by international terrorist groups and embattled governments. Students have been the victims of bombings, shooting, and kidnapping and hostage situations. In the last the forty years, there have been massacres at the Ma'a lot school in Israel, the Bahr el-Baqar school in Egypt, the Beslan school in Russia, and the Nagerkovil school in Sri Lanka. Schools in the Gaza Strip, Iraq, and Afghanistan are routinely targeted by insurgents, and, in Syria, schoolchildren are bombed by their own government, which is engaged in a worsening civil war. Mass student kidnappings became a new fear when terrorists from the al-Qaeda-linked group Boko Haram posed as soldiers to gain trust and then kidnapped more than 270 girls from their boarding school in Nigeria on April 16, 2014. Boko Haram leaders threatened to sell them into marriage and the sex trade for $12 apiece, to raise money for the cause. Boko Haram next attacked the

FIGURE 5.2 Sign found at Andrew Kehoe's home.

village where the girls were from, killing 150 family members and search-and-rescue team personnel. The Nigerian army is unable to repel Boko Haram attacks and protect citizens.

The 2004 Beslan school attack in Russia is difficult to read about, and the pictures are extraordinarily painful to view. However, to glean valuable information for hardening efforts, we must confront the harsh reality of these attacks. This case, in particular, provides insight into the mentality of terrorist groups and actors that will target defenseless children, as well as how poor response by the government to a mass hostage situation can lead to even more bloodshed.

Case Study: Siege at Beslan School Number 1—Innocence Lost (Fisk 2014)

Since the advent of modern terrorism in 1968, hostage taking is a tactic often used in terrorist operations, whether as a bargaining chip or to generate additional public fear. September 1, 2004, again proved another employment of the tactic, as over thirty Chechen Islamic militants took control of Beslan School number 1, in Beslan, North Ossetin-Alania, Russia. Terrorists stormed the school and quickly took 1,200 hostages, including 705 children. Unfortunately, the siege had a horrific ending, but only by revisiting the case can we learn how to prevent a similar massacre in our own country.

Beslan is a picturesque town of 30,000 near the beautiful Caucus Mountains. Unfortunately, the North Caucasus region also serves as a base of operation for al-Qaeda operatives, among other jihadists. The "Day of Knowledge" is the first day of the new school year in Russia, when students attending for the first time are greeted in a festival-like atmosphere, and those entering their last year are given flowers by the younger children as a sign of congratulations and good luck. On this fateful day, parents were also in attendance, pushing the population inside the school to maximum capacity. School started in Beslan at 9:00 a.m. that morning, the celebration having been pushed up an hour because of the forecasted high temperatures. At 9:20 a.m., terrorists seized the school, gathering those who could not escape and herding them inside the gymnasium. The terrorists were wearing camouflage uniforms and appeared to be Russian security forces conducting a counterterrorism drill, so the adults were initially unsuspecting of their activity. Overwhelmed by the size of the terrorist group and their firepower, the adults could do nothing but obey the orders of the hostage takers and sit through three days of unimaginable terror with the children.

SHAMIL BASAYEV

To understand the Beslan School siege, one needs to understand the group's leader, Shamil Basayev, who approved, planned, and ordered the Beslan attack. Basayev was no stranger to Russian

security forces, leading guerrilla operations against the Russian military in both the first and second Chechen Wars, and as the leader of the radical wing of the Chechen insurgency. He is in a unique position to plan attacks, intuitively understanding how forces will respond and their tactics and vulnerabilities. His goal is recognition of the independence of Chechnya and UN and Russian withdrawal from Chechnya. No stranger to large civilian hostage operations, Basayev also planned the soft target attack against 916 civilians at the Dubrovka Theater on October 23, 2002, a case study covered in Chapter 6 of this book. In addition to attacks on government buildings, Basayev also ordered the suicide bombing of two Russian Civil Aviation aircraft on August 24, 2004. He directed an attack at the Rizhskaya metro station in northeast Moscow on August 31, the day before his Beslan operation. In all, over one hundred persons were killed in these three attacks.

TACTIC: BLITZ ATTACK

On the morning of the attack, children and adults dressed in their finest clothes and arrived at Beslan School number 1. Waiting in the distance were thirty-five Chechen militants in military vehicles, ready to conduct a surprise attack on the school and, with overwhelming force, seize as many hostages as possible. With violence of action and confusion as to whether they were members of the Russian military, their plan was successful and they corralled most of the students and adults into the school's gym. Fifty people escaped and alerted police, and several were able to hide in the boiler room. Upon responding, police, who were unaware of the scope of the incident, wildly exchanged gunfire with the terrorists; five police officers and one terrorist were killed. Realizing the situation exceeded their capabilities, a call was put in to the Russian army for assistance.

The terrorists moved a majority of the hostages into the gymnasium. Then, with tactical proficiency, they began to construct defensive fortifications. They established sniper positions and had male hostages move desks and chairs around the entrances of the building to block potential counterattacks. The terrorists also placed improvised explosive devices (IEDs) in a "daisy-chain" configuration in the gymnasium, placing some in basketball hoops and above the heads of the hostages for the maximum casualty-producing effect (Figure 5.3). They tactically positioned terrorists in strategic locations throughout the school to repel an outside assault. Later in the morning, hostages, mostly children, were staged at the windows as human shields.

BLACK WIDOW INVOLVEMENT

As discussed in Chapter 3, the Chechen Black Widows are an asymmetric and formidable force in the terrorist group's arsenal. Another tactic used at the Moscow Theater siege and during the

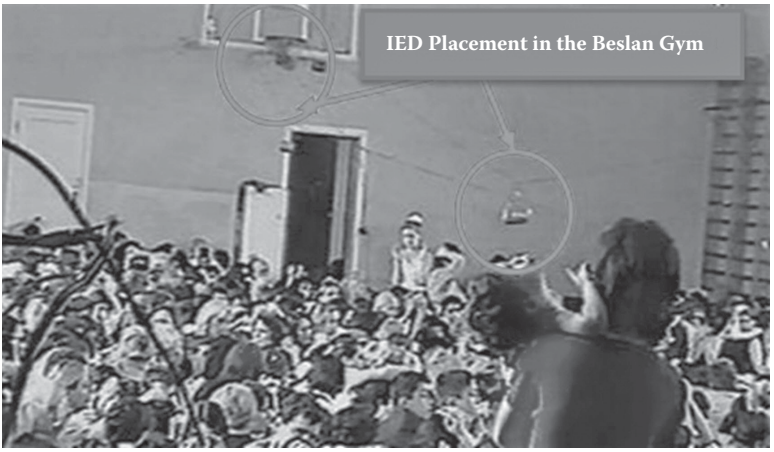


FIGURE 5.3 IED placement in the Beslan School gym.

Beslan operation was the use of female terrorists rigged as suicide bombers. By the conclusion of day 1, it is believed three of the female suicide bombers were dead. One was killed by a fellow terrorist after protesting the treatment of the hostages, specifically the children, and another died during the malfunction of her bomb. A third may have been used to detonate a bomb to kill the strongest 20 male hostages, selected by the terrorists from the group in the gymnasium. Their bodies were dumped out of a second floor classroom into the schoolyard (Chivers 2007).

PSYCHOLOGICAL TERROR

At the beginning of the siege, two male hostages were killed in front of the others in the gymnasium, their bodies dragged through the crowd. Additional threats were made by the terrorists to the government response team assembled outside the school: If any terrorist was killed by Russian security forces, fifty hostages would be executed and, if one was wounded, twenty hostages would be killed. Cell phones were confiscated to reduce the risk of hostages transmitting information to the outside, and the threat was made that anyone caught with a cell phone would be executed, as well as anyone around that person. The hostages were told that if disobedience or resistance was suspected, the hostage being disobedient would not be killed, but everyone around him or her would. Only Russian was allowed to be spoken by the hostages. To show their intent to follow through on these threats, the terrorists allowed a male to address the group. In an attempt to calm the hostages, he did not speak in Russian, and instead spoke in the local Ossetian language; he was shot and killed in front of the other hostages (Terror Operations: Case Studies in Terrorism 2007).

LOGISTICS

From the terrorists' perspective, food, water, and medical supplies were robust because they had total control of the school and its assets. They also had a large stock of ammunition and weapons; every terrorist was armed with a Kalashnikov rifle, and there was a cache of sniper rifles, RPG-7 grenade launchers, and machine guns, hand grenades, pistols, dynamite, and at least one hundred IEDs (Terror Operations: Case Studies in Terrorism 2007). The sheer amount of weaponry and the terrorists' apparent familiarity with the building led some to speculate there was on-site reconnaissance and storing of supplies during the summer while the school was being renovated (McDaniel and Ellis 2009).

The hostages were deprived of food, water, and medical supplies by the terrorists during their captivity; children and adults even had to resort to drinking their own urine. By day 3, a significant number of children and adults began showing signs of exhaustion, dehydration, and food deprivation. Many of the hostages began fainting as a result of not having any food or water and being forced to stand for lengthy periods of time. This deprivation and mental confusion was evident on day 3 when the attack and counterattack started, as some of the escaping hostages were seen running back into the school during the fighting. The terrorists were also growing weary of the standoff and became more brutal to the hostages.

DEMANDS

One of the survivors recalled her conversation with a terrorist; when she asked him why they had seized the school: "One of the terrorists said that a Russian plane flown from our airfield had killed his entire family. Now, he wanted to kill, and didn't care that it was women and children" (Leung 2005). Initial attempts to engage the terrorists in negotiations were futile; the terrorists only wanted contact with senior-level Russian officials. A request was sent for three politicians and a pediatrician as part of the negotiation team. In addition to this demand, the terrorists had made three other demands: for Russian forces to end operations and withdraw from Chechnya, for the release of militants arrested in the raids on Ingushetia, and for the United Nations to recognize their independence. On the second day of the standoff the former president of Ingushetia, Ruslan Aushev (the only one of the four people requested by the terrorists to come to the scene who did so), arrived in Beslan. Aushev had also worked on the negotiations during the Moscow Theater hostage crisis in October 2002 and was well respected in the Caucasus region.

During his meeting with the terrorist leader he secured the release of 26 hostages: 11 women (nursing mothers) and their infants. One nursing mother who had other children in the school was allowed to leave with her baby, but refused because her other children had to remain behind. She handed her baby to a terrorist, who in turn

gave the baby to Aushev (Leung 2005). Aushev was also handed a written note from Shamil Basayev with his demand. This was the only face-to-face negotiation conducted during the siege.

CNN and other news networks carried the Beslan siege live, multiplying the fear felt not only by children and parents in Russia, but also around the world. This kind of publicity is a terrorist group's dream, as they and their cause are catapulted onto the world stage. Horrific images of the aftermath of the bloody final assault are widely available on the Internet, keeping the event alive.

THE BATTLE

During the late morning on September 3, the terrorists agreed to allow medical workers into the schoolyard to retrieve the bodies of the dead thrown out of the second floor window on day 1. At approximately 12:50 p.m., four people moved toward the school yard to begin the process of retrieving the bodies; reports indicate that the terrorists fired shots at the workers, an event that had a cascading effect that would end the Beslan siege.

At 1:05 p.m, two explosions occurred in the gym, killing hundreds. It was never made clear if the explosions were caused by the terrorists or the Russian army. Fortunately, many children escaped through holes in the walls and broken windows. A full-out firefight ensued. Russian security forces detonated explosives as breaching charges to enter the gym and attempt to rescue hostages. The terrorists detonated their IEDs, setting the roof of the gym on fire; the roof collapsed, killing more of the hostages. Another breach would be conducted using a BTR-80 on the gym's western wall; this armored infantry tank fired its 14.5 millimeter machine gun as it rolled toward the school and breached the wall and the windows, likely killing more hostages.

THE CAFETERIA

While the situation in the gym unfolded, terrorists were moving the remaining children and adults, first to the hallways of the school and then to the cafeteria, which gave slight tactical advantage for the terrorists because the windows were covered with security bars. Terrorists made the women and children stand in front of the windows as human shields while Russian security forces and police fired at the building. Children and adults who were not standing in front of the windows hid in and under anything they could find; some children even hid in large pots and pans. Although they could clearly see these human shields, and women were waving white napkins and screaming not to shoot, Russian security forces, police, and local armed civilians continued to fire on the school (Chivers 2007).

The fight for the school continued, and Russian military tanks took up positions near the school and, on orders from security forces, fired 125 millimeter main gun rounds into the building

locations still occupied by the terrorists. Thirteen of the terrorists, including two women, escaped the school and hid in an outbuilding on the school property. Using tanks and Shmel rocket infantry flame-throwers, the building was destroyed and all thirteen terrorists killed. Some of the terrorists escaped the fight and tried to blend into the local population. At least one was beaten to death and another lynched by outraged family members. Some reports indicate that some of the terrorists escaped, but Russian authorities say these are rumors. Only one terrorist was captured alive; he was convicted and sentenced to life in prison.

In the end, over 330 people died at the Beslan School, including 108 children. At least 700 were wounded and required medical care. All survivors received deep psychological wounds that will stay with them a lifetime. Second only to the attacks on 9/11, the Beslan attack had the highest death toll of any terrorist attack in history.

EPILOGUE

Some of the casualties at Beslan came at the hands of the terrorists, but hundreds more occurred at the hands of responding forces. Aggravating factors included

- The apparent total disregard of hostage safety
- The use of high-caliber weapons
- Firing at human shields
- Failure to establish a perimeter cordon and allowing parents and the local population to stand near the school and even arm themselves and fire at the building
- Not having the appropriate first-response assets such as medical and firefighting support

These actions and inactions played a major role in the final, disastrous outcome of this attack.

(Source: Mr. Ralph Fisk is an emergency response and risk management expert.)

Could the Beslan siege happen in the United States? Although the likelihood of an incident on this scale, with attackers approaching a school in tanks with heavy firepower, is remote, it is quite plausible that a large-scale attack and hostage situation could occur with the help of insiders who pre-position supplies and accomplish preoperational planning. Considering that the massacre acts at Columbine, Virginia Tech, and Sandy Hook were perpetrated by amateurs, it is irresponsible to think that a preplanned, coordinated attack by a group of professionals would not result in more destruction and casualties. All types of schools, in both urban and rural areas are vulnerable. Local, county, and state law enforcement and first-responder support organizations

should exercise the possibility of a mass hostage incident in a school, reviewing the Beslan case study and fine-tuning their own response. The National Incident Management System (NIMS) is a valuable tool for preparedness, and the incident command system must be understood to prevent confusion at the scene. It is likely that if a terrorist organization is involved in a school siege, federal law enforcement will respond; therefore, prior coordination and relationship building would be extremely helpful. A list of valuable FEMA courses regarding the coordination of response is located in Appendix B.

Passive security measures, such as those discussed in Chapter 8, would be helpful at schools, including a comprehensive identification check system, and extensive background checks on all workers employed by the institution, as well as those that are contracted and subcontracted to support educational operations such as bus drivers and construction workers. Entry control points and securing points of egress are critical to repelling a school attack and catching the perpetrators. The arming of teachers might be a step toward hardening this soft target, as they could act as force multipliers during active shooter or kidnapping and hostage situations.

K–12 Vulnerability

Why are K–12 schools more vulnerable to attack? First of all, the student populace is younger and easier to overpower. Security measures are typically in place, but not consistent. For instance, as violence in our country began to rise in the 1980s, many schools began installing metal detectors at entryways. Although they work extremely well to catch weapons, school administrators found this type of screening to be time consuming, especially when trying to move hundreds of students to their classrooms every morning. Also, operating detectors or individual wands is extremely manpower intensive, so most schools abandoned the idea. The concept of school resource officers (SROs) took hold in the 1970s when protests and unrest related to the Vietnam War spilled over into school systems. SROs are sworn law enforcement officers who are detailed to the school system and work to enhance security at their institution. They may be armed and can make arrests.

However, SROs can also be of limited help when facing a determined gunman or gunmen with a practiced, solid plan and heavy firepower. For example, in the Columbine High School attack, Eric Harris and Dylan Klebold managed to kill fifteen people and injure twenty-four despite the presence of an armed guard. Jefferson County Sheriff's Deputy Neil Gardner, a fifteen-year veteran of the Sheriff's Office, usually ate his lunch with the students in the cafeteria, his car parked in front of the cafeteria doors between the junior and senior parking lots. On the day of the attacks, Deputy Gardner was eating elsewhere on campus, watching an area frequented by smokers. When shots were fired inside the

school, he pulled up to the indoor/outdoor cafeteria area where Harris and Klebold had tried to set off two bombs and had already started killing students. Gardner engaged them in a gun battle; however, he was unable to hit the perpetrators. One injured teacher and a student were able to escape during the chaos and Gardner was responsible for later saving other students as he protected them when they were fleeing. He also exchanged gunfire with the shooters when they were killing students in the library, before they committed suicide. He likely saved lives in the end, but Gardner's daily presence on the school grounds obviously did not deter the shooters from their operation. In fact, they may have purposely chosen the area where Gardner typically had lunch to start the operation, intending to kill him first and remove their only obstacle to success.

The Red Lake school massacre occurred on March 21, 2005. On that morning, sixteen-year-old Jeffrey Weise killed his grandfather, a tribal police officer, and his girlfriend at their home. Weise then took his grandfather's police weapons, vest, and vehicle, driving to Red Lake Senior High School, where he had been a student some months before. Weise first shot and killed the unarmed security guard at the entrance of the school and then targeted a teacher and five students. After the police arrived, Weise was undaunted and exchanged gunfire with them; he was wounded and then committed suicide in a vacant classroom.

In May 2014, police in Waseca, Minnesota, arrested seventeen-year-old John David LaDue on charges related to an elaborate plan to carry out a massacre at a nearby school. According to his 180-page diary, which police found in his bedroom, LaDue plotted to kill his family members, start a diversionary fire to distract first responders and then go to a nearby school. He was first going to kill the school resource officer and then set off bombs and shoot students and staff. A resident living next to a storage facility worker tipped off police to the suspicious teen; contents of his locker revealed a pressure cooker, pyrotechnic chemicals, steel ball bearings, and gunpowder. He had also stockpiled three completed bombs, an SKS assault rifle, a Beretta 9 millimeter handgun, hundreds of rounds of ammo, and a safe with several other guns at his home. LaDue tested his devices at a local elementary school playground and intended to attack the school on the anniversary of Columbine; however, it fell on Easter Sunday and school was not in session. Locals described LaDue as a polite boy who did well in school and had plenty of friends (Ford and Brumfeld 2014).

Often, the perpetrators of K–12 violence are known—current or former students, staff, or teachers. They know the school layout and class schedule, the school resource officer's habits, and when and where to strike for the least resistance and most effect. Deterring school violence under these circumstances is very difficult.

Religious elementary schools in the United States have also been the target of terrorists. In August 2011, federal law enforcement officers arrested Emerson Winfield Begolly in New Bethlehem, Pennsylvania. Begolly was a moderator and supporter for the internationally known Islamic extremist web forum Ansar al-Mujahideen English forum (AMEF). He produced and distributed a 101-page document with instructions for constructing chemically based explosives and a target list including Jewish schools (Investigative Project on Terrorism 2011). Religious schools must be especially vigilant because religious terrorism is the most dangerous, with actors believing their violent actions are sanctioned and just.

Colleges: Campus Culture and Vulnerability

Every type of bad actor now sees the university campus—facilities, programs, students, and staff—as a conduit to their illicit activities. Many cultural factors are at play that resulted in this exploitation. For instance, a basic higher education tenet is academic freedom, which allows professors and students to explore topics in an environment free of repression or censorship so they may fully participate in the learning process. Except for some instances of religious universities, this freedom also applies to research activities, where open inquiry means no query or methodology is out of bounds. Freedoms on campus are typically extended to student activities, school newspapers, and protest events, and universities are unable or unwilling to contain inciting or seditious speech. Also, formerly able to operate in a disconnected manner from society in their "ivory tower," the higher education system is more transparent than ever. Skyrocketing tuition rates and campus scandals have made parents, taxpayers, and political representatives angry and demanding disclosure. The combination of these internal and external dynamics has contributed to a very open campus environment that is rich for learning, as well as exploitation.

For example, due to the government's problems with cost overruns by major defense contractors, universities are increasingly relied upon for research and development (R&D) in sensitive areas such as cyber warfare and weapons of mass destruction, including the testing and development of chemical, biological, and nuclear weapons and counterweapons (American Association for the Advancement of Science 2014). Often, the projects involve future cutting-edge technology; therefore, schools compete for the work and associated funding and prestige. However, the mere presence of R&D activities makes the campus a target for anti-government anarchists or single-issue domestic terrorists such as animal or environmental rights activists. Annual government reports listing

R&D funding to specific schools may paint a target for foreign actors who may also attempt to penetrate the campus (American Association for the Advancement of Science 2014). Nation-state and nonstate actors are stepping up collection activities against the US industrial base, which includes campuses conducting government research (Office of the Director of National Intelligence 2011). According to the FBI, "The open environment of a university is an ideal place to find recruits, propose and nurture ideas, learn, and even steal research data" (FBI 2011).

Prevailing negative attitudes regarding security measures and agencies among our citizens may also contribute to the increase in nefarious activity in and around campuses. As time passes from the 9/11 tragedy and subsequent terrorist plots have failed or been interrupted, intelligence and law enforcement agencies fear a sense of complacency. Complicating the situation, it is important to note that the American citizen's trust in the government is at a historic low point (19 percent), and one in three people believe the government is threatening their personal freedoms with post-9/11 security activity and laws (Pew Research Center 2013). Certainly these attitudes are conveyed on campus with the younger, more activist-minded generation and faculty trying to enforce principles of academic freedom. Therefore, any security measures put into effect on campus may be met with resistance, not the compliance we expect. The school may even back down to a lower security posture to pacify students and faculty, resulting in more vulnerability.

Also complicating matters is the fact that security fatigue has set into the population as a whole, with citizens tired of looking for threats and being vigilant. Wake-up calls such as the tragic Virginia Tech murders, an event which could be characterized as "higher education's 9/11," and subsequent campus shootings have shifted security focus to weapons and student lockdown/notification procedures. Although the lone-shooter threat is compelling, campus security must be careful not to lose sight of other vulnerabilities and threats. In other words, while we are specifically looking for guns at the entrance of a classroom building, a crude but effective bomb may be under construction in the basement.

Campuses Already Under Attack

Make no mistake: our schools are already under persistent passive attack. For instance, foreign intelligence services (FISs) and nonstate actors continuously prey on campuses to steal intellectual property and bypass expensive research and development. Also, FISs are actively recruiting students and professors for espionage and to use later as sources, with multiple cases on college campuses in the last five years and actors exhibiting increasingly bold tactics (FBI 2011).

The case of University of Tennessee professor Dr. John Reece Roth illustrates lack of policy and procedure, and how the open academic

environment is penetrable by "countries of interest." Despite statutory requirements, Roth was able to hire foreign national students from China and Iran to work on his classified, Department of Defense-funded plasma-related aerospace project on campus. The students recruited him, and he traveled at least eight times with sensitive material to China (FBI 2009). Roth is not the type of professor we might expect would be susceptible to this type of FIS activity; he was in his late sixties when approached by the students, an emeritus professor of electrical engineering who taught at Tennessee for nearly thirty years after his time at NASA. He also holds eleven patents and testified before Congress on nuclear fusion. Roth was coerced into thinking that intellectual property should be open and available to all countries. Roth's academic colleagues feel that his ego was stroked by attention from the students and host government and that he believed he was making a significant intellectual contribution to the world (Golden 2012).

Intellectual property theft is not the only goal of foreign governments operating on our campuses. The 2009 case of Russian spy Lidiya Gurveva (using the name Cynthia Murphy) is particularly illustrative of how the campus environment can be exploited merely to collect information on professors and students. Gurveva was pursuing an MBA degree at Columbia Business School, Columbia University, in 2008 when her handlers gave her the following assignment:

> [S]trengthen…ties w. classmates on daily basis incl. professors who can help in job search and who will have (or already have) access to secret info…[r]eport to C[enter] on their detailed personal data and character traits w. preliminary conclusions about their potential (vulnerability) to be recruited by Service.

They also directed Gurveva to "dig up personal data of those students who apply (or are hired already) for a job at CIA" (US Department of Justice 2010). In yet another campus spying case, Andrey Bezrukov (also known as Donald Hatfield) was arrested in June 2010 for being an agent of Russia. He graduated from Harvard's Kennedy School of Government and, while a student, developed associations with professors at George Washington University and Oxford University. Bezrukov/Hatfield targeted a professor who was once former Vice President Albert Gore's national security advisor, as well as other policymakers at Kennedy School reunions and think-tank events (Srivatsa and Zu 2010). These cases clearly illustrate the vulnerability of professors and students to recruitment and the ease with which foreign nations can penetrate our universities.

Cybercriminals are also present on campus; data theft is an emergent challenge as servers are breached to steal student information protected by law, putting the university at great risk and liability. For example, the

University of Maryland regretfully announced in February 2014 that information had been stolen from its database since 1998 on 300,000 students and faculty who were issued identification cards (University of Maryland 2014). Although Maryland's breach may have been due to failure to protect onsite servers and recognize ongoing penetration activities, many universities are now moving their electronic student, faculty, and staff records to the virtual servers offered in the "cloud"—which presents new and significant vulnerabilities.

As if spying and cybertheft are not enough of a challenge for university security officials, campuses are increasingly seen as a "safe haven" for drug dealers. The activity is not what we might expect, such as students attempting to grow marijuana in their dorm rooms or selling dime bags at parties. Police are now discovering methamphetamine labs on college campuses, which not only pose health dangers to students, but also place explosive materials in high-occupancy buildings and bring an unwanted, dangerous element to campus property. In 2013, the cases were not just confined to urban settings, and it seems no university is now immune from this emergent threat. For example, meth labs were discovered in dormitory rooms at Georgetown University, in a music practice room at Southern Methodist University, and on the roof of an on-campus student apartment building at the College of Charleston.

Finally, the J-1 Student Visa Program has been repeatedly misused and exploited, notably by nineteen convicted terrorists since 1990, including Mohammed Atta, leader of the 9/11 cell (Kephart 2005). Over 100,000 foreign students enter the United States annually on student visas, but not all of them actually show up or stay at school. Despite new, rigorous post-9/11 laws to scrutinize requests and follow up after visa expiration, many still slip through the cracks. In 2006, eleven Egyptians with J-1 visas did not appear for class at the University of Montana. The school waited 48 hours after classes began to report the absence to the FBI, which then started a resource-intensive manhunt to find the eleven (workpermit.com 2006). Not all were captured.

The J-1 visa has also been used as a conduit to attain asylum. The case of Ibragim Todashev, friend of Boston Marathon bomber Tamerlan Tsarnaev and admitted murderer of three people in Massachusetts, is compelling. A Chechen, Todashev came to the United States on a J-1 visa and, instead of attending college, immediately applied for asylum and, later, citizenship. He was on a downward spiral with a lengthy criminal record, yet his newly obtained citizen status protected him from deportation. Todashev was killed by law enforcement when he attacked investigators during an interview to collect evidence regarding the Boston bombings and the triple murder in Massachusetts. The University of Massachusetts-Dartmouth also became part of the bombing investigation because coconspirator Dzhokhar Tsarnaev was living in his dorm

room and storing evidence in his closet at the time of the event. Although Tsarnaev had failed seven classes in the previous three semesters, was carrying $20,000 in student debt, and was a known marijuana smoker/distributor, he was allowed to remain on campus, a decision the university likely regrets today (Goode and Kovaleski 2013). These cases show how university policy decisions can result in vulnerabilities.

In another case, Khalid Ali-M Aldawsari, a Saudi student studying chemical engineering at Texas Tech University, was arrested in February 2011 on a charge of attempted use of a weapon of mass destruction. A notebook was found at Aldawsari's residence indicating he had been planning to commit a terrorist attack in the United States for years. One entry describes how he sought and obtained a particular scholarship because it allowed him to come directly to the United States and helped him financially, which he said "will help tremendously in providing me with the support I need for Jihad" (US Department of Justice 2011). The journal goes on to say: "And now, after mastering the English language, learning how to build explosives and continuous planning to target the infidel Americans, it is time for Jihad." Aldawsari had the blueprints of chemical IEDs and had already started purchasing the components for his weapons. Targets included former US military personnel, a nightclub, dams, and nuclear power plants.

Escalating Number of Attacks on College Campuses

Perhaps inspired by successful school attacks abroad, terrorists are now turning their sights toward our universities. El Mehdi Semlali Fahti, 27, came to the United States from Morocco in 2008 on a student visa. However, he flunked out of Virginia International University and the visa expired. Fahti traveled across the county and was arrested for a trespassing charge that was dismissed, turned over to immigration officials in Virginia, and placed in custody. However, he was able to stay in the United States after manufacturing a story about imprisonment and beatings by Moroccan police. A judge was persuaded to approve his request for political asylum in 2011. Fahti traveled to the West Coast, and was arrested for theft in California; while serving his sentence, his case was again turned over to the immigration agency, but a judge released him from custody in August 2013 (Investigative Project on Terrorism 2014d).

Fahti moved to Connecticut and by January was plotting to attack a university and a federal building using remote-controlled hobby planes packed with explosives, components of which he had started to gather. Fahti was living in an apartment in Bridgeport, Connecticut, with a man he met while incarcerated in Virginia. Fahti told undercover FBI agents, who thankfully became aware of his plot during a sting operation, that he had studied the plan for months, had learned how to pack the explosives while he was a student in his home country, and would be able to

obtain the materials at the Mexican border. He also said the plot would be funded through "secret accounts" that used laundered cash and drug-dealing profits. In a conversation with the FBI, Fahti says "the more he thinks about the case, he laughs because he cannot believe the judge believed him" and allowed him to stay in the United States for political reasons (Mayko 2014). He also stated that three things cause fear in the American people: causing harm to schools, the economy, and their sense of security (Investigative Project on Terrorism 2014c).

The J-1 "summer study program" visa is now being exploited by human traffickers and so-called labor recruiters to bring young would-be students to the United States to participate in illegal or immoral activities. The problem came to light in 2010, when law enforcement officials found would-be students in Myrtle Beach, South Carolina, working in strip clubs, crammed into dirty apartments, eating at food kitchens, and even begging on the street. Summer study students are also recruited by the adult entertainment industry and have been used to smuggle cash and other goods back to their home country by criminal groups (Weiss, Baker, and Mohr 2010). The hopeful students' passports are seized upon entry to the United States and they are threatened into complying with the trafficking groups. Some students do attend programs on campuses, possibly introducing the criminal element.

Terrorist attacks on college campuses are increasing worldwide. In the United States, 2005 University of North Carolina-Chapel Hill honors graduate Mohammed Reza Taheri-azar sought to "avenge the deaths of Muslims worldwide" and to "punish" the United States government. In March 2006, he drove a rented sports utility vehicle into a crowd of students with the intent to kill. Although no one was killed in the attack, nine people were injured (none seriously). Taheri-azar was born in Iran, but moved to the United States at the age of two, growing up in North Carolina. He pled guilty to nine counts of attempted first-degree murder, and in 2008 was sentenced to 33 years in prison, on two counts of attempted murder. In one letter, Taheri-azar wrote, "I was aiming to follow in the footsteps of one of my role models, Mohamed Atta, one of the 9/11 hijackers, who obtained a doctorate degree" (Schuster 2008).

The deadly al-Qaeda splinter Boko Haram is actively targeting colleges in Nigeria in its campaign of fear; in 2013, gunmen entered the male dormitory in the College of Agriculture in Gujba, killing forty-four students and teachers in their sleep. This is not a new tactic for Boko Haram; the group was also responsible for a night massacre at a technical college in 2010.

Bad Blood: Intelligence, Law Enforcement, and Higher Education

There is a possibility action (or nonaction) by security agencies may be contributing to campus vulnerability to domestic and foreign bad actors.

Unfortunately, the historically poor relationship between academia and intelligence and law enforcement agencies has led to difficulty with their partnering to address vulnerabilities and threats on campuses. This "bad blood" dates back to 1956 with the FBI's Counterintelligence Program (COINTELPRO), a series of covert projects in which the Bureau conducted surveillance and disruption activities against domestic political organizations on campuses (Churchill and Vander Wall 2002). COINTELPRO infiltrated college campuses to monitor antiwar activity during the Vietnam War and, when this activity came to light in 1971, massive protests erupted on campuses, impacting the relationship between academia and the government.

Activities on campus by the Central Intelligence Agency (CIA) from 1967 to 1973 further strained the relationship. Operation CHAOS was the code name of a CIA domestic espionage program to unmask possible foreign influences on the student antiwar movement on campuses (Rafalko 2011). Project RESISTANCE was a parallel operation, in which the CIA worked with college administrators, campus security, and local police to identify antiwar activists and political dissidents without any infiltration taking place (Church Committee Reports 1975).

A review of official documents regarding COINTELPRO, CHAOS, and RESISTANCE, especially the Church Committee proceedings, yields great data regarding interaction between higher education and intelligence agencies during a period of extreme domestic unrest. Present-day concerns about government and law enforcement activities on campus re-emerged in 2011, when it was revealed the New York Police Department had infiltrated colleges to monitor Muslim students and activities (Hawley and Apuzzo 2011). This case was a lightning rod for the media and led to state-by-state cases of intelligence community activity on college campuses documented by the American Civil Liberties Union (ACLU) in 2011 (ACLU 2014).

The literature regarding attitudes toward, perceptions of, motivation for, resistance to, and barriers to the relationship between higher education and the intelligence community highlights the cultural disconnects of two enterprises that essentially share the same goal: protecting First Amendment rights and national security. In terms of the intelligence perspective, the FBI 2011 white paper entitled "Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education" gives great insight into the subject. The higher education view on the tenuous relationship comes into view through an essay in the *Chronicle of Higher Education* entitled "Academics and National-Security Experts Must Work Together" (Gansler and Gast 2008). In this article, the authors discuss legislative and environmental changes since the 9/11 terrorist attacks and the impact on higher education. They also address the cultural divide

between higher education and intelligence agencies, asserting that it is "so often at the root of poor policies and unnecessary roadblocks for both groups" (Gansler and Gast 2008). This balanced essay asserts that experts in the intelligence field don't fully understand how communication with other countries is crucial to scientific research, and universities and research institutions fail to appreciate the importance of securing technology and protecting sensitive information. Finally, an analysis of the impact of the Economic Espionage Act of 1996 gives insight into how what was supposed to be a framework for success is not working to protect the academy (Brenner and Crescenzi 2006).

The institutions of higher education and the intelligence community have both witnessed great change and turmoil in light of the 9/11 terrorist attacks on our country. The events of 9/11 and subsequent investigations into the campus-related activities of the hijackers, new statutory reporting requirements, and continued, persistent collection on campuses by "countries of interest" have potentially aggravated an already strained relationship between the two enterprises. Both have undergone institutional reform, forced by uncontrollable environmental conditions, and both are inherently resistant to change. Due to the urgent nature of national security concerns following 9/11, there was no time to plan strategically for the change, to seek mutual agreement, or to communicate cross enterprises properly. The situation continues to evolve with current events and emergent challenges; therefore, an opportunity exists to bridge the gap and to partner strategically for future change events.

In response to increased concerns, the FBI created the National Security Higher Education Advisory Board (NSHEAB) in 2005. The NSHEAB consists of nineteen university presidents and chancellors and strives to meet on a regular basis to discuss national security matters that intersect with higher education. Previous panels included discussion on protection of weapons of mass destruction research and laws regarding domestic terrorism investigations on campuses. However, the NSHEAB has become much less engaged over time. The Department of Homeland Security instituted the Homeland Security Academic Advisory Council (HSAAC) in March 2012 to discuss matters related to homeland security and the academic community, mainly issues regarding security-related curriculum, recruitment of students to DHS, academic research, and cybersecurity on college campuses.

One of the subcommittees deals with campus resilience. The Resilience Pilot Program (CR Pilot) was launched in 2013 for seven select US colleges and universities to help them take proactive steps to enhance preparedness and campus resilience. The CR Pilot is a joint initiative of DHS's Federal Emergency Management Agency (FEMA), the US Immigration and Customs Enforcement Student and Exchange Visitor Program, and the Office of Academic Engagement. The CRP will harvest best practices,

lessons learned, and resources to help schools identify their vulnerabilities and be more resilient and prepared. Drexel University, Texas A&M, and others are participating in the project (DHS 2013).

In Chapter 9, we discuss hardening efforts for colleges that include strengthening partnerships with law enforcement and harvesting best practices from around the country.

Churches

Churches are another soft target where violent attacks are met with disbelief, especially when perpetrated by an actor with an extreme religious ideology. How can anyone's God condone the killing of another human being? We also now have a "black swan" phenomenon of Christians killing Christians and Muslims killing Muslims in the name of their extremist religious ideology. The worship space, formerly respected and shielded from violent crime, has been infiltrated by criminals and murderers, whether as a place to exact personal revenge against a parishioner, to steal money or artifacts to pay for drug buys, or to carry out an attack in which the institution and ideology are a target.

Despite these cultural changes, clergy may not see security of their building and faith community as a pressing issue. A survey conducted by LifeWay Christian Resources posed questions to more than 1,300 evangelical leaders from around the world to gather information about what they considered their most urgent concerns. The results of the survey, which included topics related to faith and life in modern society, did not return any concerns about safety, security, or terrorism. Carl Chinn, a church security expert, has been tracking US church-related crimes and statistics since 1999. Deadly force incidents (DFIs) include abductions, attacks, suspicious deaths, suicides, and deadly force intervention/protection. Between January 1, 1999 and February 1, 2014, Chinn reports 792 DFIs at faith-based organizations, with 286 episodes resulting in deaths. Almost 54 percent of DFIs were related to domestic violence, personal conflict, and robbery; guns were the weapon of choice (472 incidents) followed by knives (141 incidents) and explosive devices/Molotov cocktails (48 incidents). There were forty-two incidents related to what Chinn labels "religious bias" (Chinn 2014).

Chinn also points out there is no government organization responsible for tracking crimes specifically associated with churches. Following up on the LifeWay survey and data compiled by Chinn, Brian Gallagher, a former member of the US Secret Service and church security expert, interviewed a church planting organization about its perspective on safety and security related to its family of 100 churches in the United States. This particular organization, which asked to remain anonymous,

revealed less than 10 percent of their churches invested funds to provide proper security for their facility. The majority of the churches in the organization had never considered security or terrorism as a concern to their congregations (Gallagher 2014).

The advent of "megachurches" in the United States has presented a unique vulnerability: there are fewer worship sessions, but they are attended by thousands of attendees. Lakewood Church in Houston, Texas, is the largest megachurch, with over 16,800 worshippers attending popular author Joel Osteen's services at the former Compaq sports arena (Figure 5.4). Although the church has a high-tech security camera system and around-the-clock guards including off-duty law enforcement officers, it is still vulnerable. On March 9, 2014, possibly during services, a safecracker stole over $600,000 in collection money. Lakewood generates $75 million in revenue annually, making it a lucrative target for theft. Nationally, thefts of money and securities constitute a significant problem for churches. Wisconsin-based Church Mutual Insurance Co., which insures about 95,000 churches, reported 178 such thefts in 2013. That total declined from 240 cases in 2011, but the value of money stolen rose to more than 9 percent of total theft claims paid (Turner and Hlavaty 2014).

Churches also have a unique vulnerability: they invite wayward members of society to worship, for counseling, or to attend support

FIGURE 5.4 The Lakewood megachurch.

groups. This exposure is difficult to mitigate, although Chapters 8 and 9 discuss additional steps clergy and staff can take to secure the facility and populace. However, unlike school attacks, many church crime perpetrators have no association at all with the church; they have never attended a service and do not know the clergy members or parishioners. Therefore, the church attack may be more about opportunistic crime or could just serve as a symbolic target. The outward appearance of a hardened facility is therefore extremely important so that the terrorist or violent criminal shifts his or her intentions elsewhere.

The Proliferation of Church Attacks

Church attacks are common around the world, and many are perpetrated by enemies common to the United States. For instance, in Kenya, Christian churches are routinely targeted by radical Islamist terrorists from the Somalia-based al-Qaeda splinter group al-Shabaab. Tactics include use of bombs, semiautomatic weapons, or even machetes. Kenya is a natural target for terrorists; it has East Africa's biggest economy, is Westernizing, and is a recipient of US counterterrorism funding. Also, the Nairobi government has sent troops into neighboring Somalia as part of an African Union force (AMISOM) to combat al-Shabaab, drawing their wrath. Christianity is the predominant religion in Kenya also making it a target for those with a radical Islamist ideology. In Nigeria, Boko Haram militants routinely target churches, often walking in doors closest to the altar and using semiautomatic weapons on stunned worshippers for maximum death in a short period of time.

A recent case in England perfectly illustrates how a terrorist can enter a foreign country and quickly move to the execution stages of an attack against churches. Twenty-five-year-old white supremacist Pavlo Lapshyn, a Ukranian citizen, was a PhD student who won a competition for a work placement with Delcam, a specialist software firm in Birmingham, UK. However, Lapshyn never intended to work; the competition merely facilitated his plan to carry out hate crimes against Muslims in the United Kingdom. He practiced building and detonating hexamethylene triperoxide diamine (HMTD) devices packed with nails in the Ukraine and researched how to buy similar bomb components in Birmingham. He flew to England on April 24, 2013, on his work visa and had been in the country only five days when he started a campaign of terror. His first victim was 82-year-old Mohammed Saleem killed by Lapshyn as he walked home from evening prayers at a mosque in Birmingham. On June 21, Lapshyn planted explosive devices in a child's lunch box at the mosque gates, and seven days later, he placed a bomb on a roundabout near Wolverhampton Central Mosque. The most serious attack was on July 12 at the Tipton mosque, where Lapshyn packed hundreds of nails in a bomb on a railway embankment next to its car

park and detonated it during what he thought was the prayer service. Thankfully, mass casualties were averted because, unbeknownst to Lapshyn, prayers were held an hour later than usual, so parishioners had not yet arrived. Using forensics from the scene and a shadowy picture of Lapshyn from CCTV, police were finally led to his workplace at Delcam, and his apartment and a trove of evidence. Lapshyn is serving a forty-year prison sentence for the killing and the bombings. Interestingly, he was on police radar in Ukraine, where his flat was damaged in 2010 by a chemical explosion that he told authorities was related to his school work in a lab project gone bad. Yet no travel restrictions were imposed and he was not being watched by authorities. The case illustrates how a perpetrator can go from planning stages to execution in a short period of time, even days after entering a foreign country. Police in the UK were on Lapshyn's trail during his attack spree, but the investigation was difficult and he was able to continue his operation (Lumb and Casciani 2013).

Shared religion or nationality is not a deterrent when selecting targets. For example, in 1993, members of the Italian Mafia (presumably Catholic) bombed two of Rome's most venerable Catholic churches—San Giovanni and San Giorgio—to further their political goals. In our country, right-wing religious extremist Christians have killed other Christians without second thought to advance their goals. Islamist extremists have bombed mosques in Libya, Nigeria, and Mali. Even historic mosques and tombs, revered by Muslims, have also been targeted. For instance, the world was stunned in July 2012 when terrorists from the al-Qaeda splinter group Ansar Dine bombed the Yahya mosque in Timbuktu, a UNESCO World Heritage site. They even pried open a fifteenth century door, which many Muslims believed was supposed to be closed until the end of the world and the return of the prophets. In 2006, Wahhabi militants who bombed the Askariyyah shrine in Samarra, Iraq, almost ignited a civil war. The shrine houses the graves of the 10th and 11th holy imams, descendants of Muhammad. In 2014, members of al-Qaeda splinter ISIS destroyed the tomb of the prophet Jonah (in the Old Testament as being swallowed by a whale) in Mosul, Iraq. These "crimes against history" are shocking, get widespread press coverage for a group, and can shift the core of a conflict. Therefore, asymmetric attacks on a church by members with similar religious beliefs should not be discounted.

US Churches as Targets

Unfortunately, terrorists have taken a page from the international playbook and are now targeting US churches. Levar Haley Washington, Gregory Vernon Patterson, Hammad Riaz Samana, and Kevin James were arrested in August 2005 and charged with conspiring to attack synagogues and other targets in the Los Angeles area. Kevin James allegedly founded Jamiyyat ul-Islam Is-Saheeh (JIS), a radical Islamic prison

group, and converted Levar Washington and others to the group's mission. The JIS allegedly planned to finance its operations by robbing gas stations (Zuckerman 2014). The men were convicted and their sentences ranged from five to twenty-two years in federal prison.

In the 2009 "Bronx plot," James Cromitie and his three accomplices separately converted to Islam while in prison. After meeting at the Masjid al-Ikhlas mosque in Newburgh, New York, following their release, the men devised a complex plan to bomb the Riverdale Temple and Jewish Center in New York City and, using Stinger surface-to-air guided missiles, shoot down military planes flying out of a nearby air base. Each man is serving a twenty-five-year sentence (Investigative Project on Terrorism 2014c).

In October 2010, two packages shipped from Yemen to Chicago-area synagogues contained explosive materials of the same type used by airline attackers Richard Reid ("shoe bomber") and Umar Farouk Abdulmutallab ("underwear bomber"). The packages contained printer cartridges filled with explosive material and were intercepted while in transit on cargo planes in the United Kingdom and Dubai from intelligence tips from Saudi Arabian authorities. The Yemen-based al-Qaeda in the Arabian Peninsula (AQAP) claimed responsibility (Zuckerman 2014).

In May 2011, Ahmed Ferhani of Algeria and Moroccan-born Mohamed Mamdouh, a US citizen, were arrested by the New York Police Department after attempting to purchase a hand grenade, guns, and ammunition to attack churches and synagogues in Manhattan. The men planned on disguising themselves as Orthodox Jews in order to access the facilities. Ferhani, the mastermind of the plot, also sold Percocet, cocaine, and marijuana to finance weapons for the attack. Both pled guilty and are serving five- to ten-year terms (Investigative Project on Terrorism 2014a).

Amine El Khalifi, a Moroccan citizen illegally in the United States, was arrested in February 2012 on charges of plotting to attack the US Capitol. Before choosing the Capitol building as a target, Khalifi had proposed targets including DC office buildings, restaurants, and synagogues. He believed undercover FBI agents were al-Qaeda operatives and revealed his plots, even showing them his practice detonating test bombs with cell phones. He was arrested as he left his parked car next to the Capitol building with a bomb that was, unbeknownst to him, inert (Investigative Project on Terrorism 2014b). Khalifi was sentenced to thirty years in prison.

The worst attack against a place of worship in the United States occurred on August 5, 2012, when Wade Michael Page fatally shot six people and wounded four others at a Sikh temple in Oak Creek, Wisconsin. Page was an American white supremacist and US Army veteran with ties to white supremacist and neo-Nazi groups. He was part of the white power music scene and openly spoke and sang about the

impending racial holy war. Page committed suicide after he was shot by a responding police officer. Sikh men are often confused with Muslims due to their beards and turbans, and they have been the targets of multiple hate crimes in the United States since the 9/11 terrorist attacks (BBC News 2012).

Throughout history, churches have been a place of sanctuary and refuge for those in need. They have been targeted before, however; during World Wars I and II, hundreds of churches and cathedrals in Europe were destroyed, whether purposely hit by the enemy or destroyed by collateral damage. During the ongoing religious and political wars in myriad foreign countries, churches have similarly been affected. However, the mere idea of a church being affected by crime and terror seems new and surprising to the US populace. The unwillingness to believe a church could be a target creates a large blind spot and gives the advantage to those who wish to do us harm in shocking ways. Our churches are being targeted; therefore, security must move closer to the top of concerns for US clergy and staff.

Hospitals

Violent crimes in hospitals are typically along the lines of assault, drug theft by armed perpetrators, and gang-related violence. In addition to these criminal activities, there is discussion in the counterterrorism community about the possibility of terrorists stealing radioactive material found in hospitals in order to make a "dirty bomb." But what about the hospital itself as a target?

Hospitals are considered a critical infrastructure/key resource (CI/KR) under the national response framework, making them high-priority targets. CI/KRs are defined as individual targets whose destruction "could create local disaster or profoundly damage our nation's morale or confidence." In a multistage attack, taking hospitals and medical personnel out of play would surely lead to an increased casualty count. A terrorist attack against a hospital has not happened in the United States yet; however, these heinous assaults routinely happen in other parts of the world. Either the hospital itself is targeted or it is targeted after an event as a secondary or tertiary attack when the wounded are being rushed into the building.

As covered in Chapter 2, terrorists are often underestimated in terms of intelligence, and many have formal education. In this new type of warfare, those entrusted to save and protect lives have actually been the trigger pullers. Consider the perpetrators of the June 30, 2007, attack at Scotland's Glasgow Airport and the failed bombings in London's nightclub district two days before. Four of the seven perpetrators in the

terrorist group were physicians, two were in medical school, and one had a PhD in engineering. A hospital was also in their crosshairs; on the afternoon of July 1, police carried out a controlled explosion on two cars in the parking lot of the Royal Alexandra Hospital, where the suspects worked and had apparently intended to attack.

On November 29, 2008, members of the al-Qaeda affiliate, Lashkar-e-Taiba (LeT), began their four-day assault in Mumbai, India. The twelve coordinated shooting and bombing attacks shocked the world and lasted four days, killing 164 people and injuring hundreds. Targets included a train station, a Jewish community center, the Taj Mahal Hotel, and the Oberoi Trident Hotel. Overshadowed by the horrific events at these locations, not much has been written about one of the main targets in Mumbai: the Cama Hospital for Women and Children. The LeT terrorists specifically attempted to gain access to the maternity ward, after killing two security guards with an AK-47 and grenades at the entrance. The security doors of the ward kept them from entering, and scared patients barricaded and refused to open up, despite threats from the terrorists. The shooters wandered other hospital floors, killing other security guards and workers. When directly confronted, a frightened hospital orderly offered the shooters water; they took a drink before killing the man (IBN Live 2008).

The Tehrik-i-Taliban Pakistan (TTP), or the Pakistani Taliban, is a designated terrorist group that specializes in hitting soft targets. TTP has already tried to attack soft targets inside the United States, most notably through the failed Times Square bombing. In an example of a secondary attack against a hospital, TTP militants in Pakistan's restive province of Baluchistan first bombed a bus carrying female college students, killing fourteen. The perpetrator was a female suicide bomber, who boarded the bus with the students and then carried out the attack. At the Bolan Medical Complex, a second suicide bomber sat in the reception area of the emergency room, waiting for the right moment to attack. As dead and injured bus victims were brought into the emergency room and parents and local officials gathered, he detonated his vest, killing eleven (*The Telegraph* 2013). Heavily armed militants then stormed the hospital, taking hostages and shooting from the windows, killing several police officers and local officials.

Other coordinated, violent attacks against hospitals by the TTP in the last few years include the 2008 DI Khan Hospital attack (thirty-two dead) and the 2010 attack against the Jinnah Postgraduate Medical Center in Karachi (thirteen dead). The resurgent Taliban in Afghanistan has also attacked that country's hospitals; the worst attack to date occurred in 2008, when a lone suicide bomber struck in the cafeteria at the Kabul hospital, killing six people and injuring twenty-three during a surgery training session. The hospital is located in the "green zone,"

FIGURE 5.5 An al-Qaeda gunman lobs a live grenade at a group of civilians in a Yemeni hospital. (McCluskey, Brent. "Graphic CCTV Footage of Militant Attack in a Yemeni Hospital." podcast audio2013, http://www.guns.com/2013/12/14/graphic-cctv-footage-militant-attack-yemeni-hospi tal-video/, 2013.)

heavily guarded, and very close to the US embassy. Also in Kabul, three Americans were killed on April 24, 2014, when a security guard opened fire at a hospital funded by a US Christian charity, killing a father and son who were visiting from the United States and a doctor.

A brazen attack by al-Qaeda in the Arabian Peninsula (AQAP) against a hospital in Yemen on December 5, 2013, stunned the world (Figure 5.5). The primary target was a nearby defense building; however, stray militants entered a nearby hospital, killing two German and two Vietnamese doctors, and one Indian and two Filipino nurses during the assault. Most were executed in front of the staff. The attack was captured on closed-circuit television footage and broadcast by state media, causing widespread outrage among Yemenis, as AQAP has portrayed itself as fighting for the average citizen against foreign drone strikes. Whether outraged or sensing a rift between the citizens and AQAP, a member of the core al-Qaeda group issued the following apology: "We do not fight in this way, and this is not what we call on people to do, and this is not our approach. We warned fighters not to attack the hospital."

Here in the United States, we have had a few indications that hospitals might be in the terrorist crosshairs. In November 2002, the FBI issued an alert to hospitals in San Francisco, Houston, Chicago and Washington, DC, warning of a vague, uncorroborated terrorist threat. In August 2004, the FBI and DHS issued a nationwide terrorism bulletin that al-Qaeda might attempt to attack Veteran's Affairs hospitals throughout the United States, and in April 2005 the FBI and DHS investigated unusual incidents of imposters posing as hospital accreditation

surveyors. The Joint Commission on Accreditation of Healthcare Organizations sent a security alert to hospitals.

Nefarious Use of Ambulances

Ambulances are being used in conflicts as vehicle-borne (VB) IEDs (Pakistan in 2013), as shooting platforms (Gaza in 2001), to move terrorists (Pakistan in 2004), to hide suicide belts (Gaza in 2002), and as getaway vehicles (Gaza in 2004). We have much to learn from these case studies in terms of hardening our hospitals to protect ambulances from theft, enhancing our laws regarding re-selling first-response vehicles, and educating first responders on the threat.

Terrorists have used ambulances as VBIEDs in creative ways. January 12, 2013 was a deadly day in Quetta, Pakistan, with 103 people killed and over 200 wounded in four separate, coordinated, and planned soft target attacks by the TTP. First, there was an attack at a mosque that killed twenty-two worshippers, followed by a mass shooting at a recreational area used by Pakistan's military commandos, with another twelve dead. Next, a suicide bomber detonated his vest at a billiards hall packed with families. As police officers, journalists, and rescue workers rushed into the building, a second blast emanated from a bomb hidden in a stolen ambulance that had folded itself into the pack of response vehicles. The total death toll at the billiards hall was sixty-nine (Associated Press 2013).

The Taliban in Afghanistan has also used ambulances extensively in its attacks. For example, on April 7, 2011, Taliban suicide attackers used an ambulance VBIED to attack a police training center in the southern province of Kandahar. If actual ambulances are not available, groups will simply create one for the attack. In January 2010, the threat of cloned first-response vehicles came to light when, during coordinated attacks in downtown Kabul, the Taliban detonated a VBIED in a van disguised as an ambulance.

The international terrorist group Hamas is expert at using ambulances. On May 11, 2004, an Israeli television station aired footage of armed Arab terrorists in southern Gaza using an ambulance owned and operated by the United Nations to support Palestine refugees. Palestinian gunmen commandeered the emergency vehicle as getaway transportation after murdering six Israeli soldiers in Gaza City. The footage shows two ambulances with flashing lights pulling onto a street. Shots and shouts rang out during the nighttime raid, and then a gang of militants piled into one of the ambulances, clearly marked "UN" with the agency's blue flag flying from the roof, and sped away from the scene (Malkin 2004).

Consider how often first responders leave ambulances idling at the scene or at the hospital entrance. There have been reports of ambulances stolen in the United States and some were never recovered. But if a bad

Ford: E-Series Van CHATEAU 1979 ford chateau e 350 **Ambulance**

11h left
Friday, 12 AM

$1,075.00
6 bids

2002 Ford E 350 Box **Ambulance**

$4,999.00
or Best Offer

12 Watchers

1994 E 350 diesel **Ambulance** Runs Great!

14h left
Friday, 3 AM

$2,025.00
17 bids
$3,500.00
By it Now

FIGURE 5.6 Ambulances for sale at an online auction site.

actor does not want to steal an ambulance or build a clone, it is now possible simply to buy one on the Internet. Cash-starved communities often sell their old emergency response vehicles to fund a new fleet. Websites such as Ambulance Trader and Fire Truck Trader could be exploited by terrorists and criminals flush with cash who want to make a quick buy (Figure 5.6). Ambulances are now for sale on eBay and payable in full through PayPal, a nonbank that can be funded anonymously (Hesterman 2013).

Recognizing the growing threat, DHS issued an advisory in 2013, entitled *Terrorist Tradecraft: Impersonation Using Stolen, Cloned or Repurposed Vehicles,* with the following guidance:

- Mitigating the risk:
  - Secure station or facility entrance and exit points, including apparatus bay doors

- Limit or lock unattended emergency vehicles
- Establish a policy for decommissioning vehicles
- Stay current on the "branding" of vehicles used by neighboring jurisdictions and mutual aid companies
- Consider using holograms on emergency vehicles for authentication
- Establish a stolen vehicle reporting process that includes "be on the lookout" warnings for high-interest vehicles

- Possible indicators:
  - Improperly marked emergency vehicles
  - Driver of emergency vehicle not knowledgeable about area of responsibility or service
  - Incorrect vehicle decal verbiage, colors, word font, and size
  - Visible identifiers such as phone numbers, license plates, or call numbers that are inconsistent with the vehicle's operating area or mission
  - Heavily loaded vehicle, possibly beyond capacity

In conclusion, schools, churches, and hospitals are places where citizens should feel safe and be protected from danger. Unfortunately, world events indicate an escalation in the number of attacks and scale of violence against these soft targets. We are also no longer safe in the places we go for relaxation and entertainment; the next chapter explores the rising threat against shopping, sporting, and other recreational venues.

REFERENCES

ACLU (American Civil Liberties Union). "Spying on First Amendment Activity—State-by-State" (2014).

American Association for the Advancement of Science. "Guide to R&D Funding Data—R&D at Colleges and Universities" (2014).

Associated Press. "Bombings Kill 103 in Pakistan," news release, http://www.nydailynews.com/news/world/bombing-pakistan-billiard-hall-kills-69-article-1.1237569 (2013).

BBC News. "Profile: Wisconsin Sikh Temple Shooter Wade Michael Page." http://www.bbc.co.uk/news/world-us-canada-19167324 (August 7, 2012).

Brenner, Susan W. and Anthony C. Crescenzi. "State-Sponsored Crime: The Futility of the Economic Espionage Act." *Houston Journal of International Law* 28(2) Winter 2006.

CDC (Centers for Disease Control and Prevention). "Schools and Terrorism: A Supplement to the National Advisory Committee on Children and Terrorism Recommendations to the Secretary." Atlanta, GA, 2003.

Chinn, Carl. "Ministry Violence Statistics." http://www.carlchinn.com/Church_Security_Concepts.html

Chivers, C. J. "The School." *New York Times,* March 14 (2007).

"Church Committee Reports" (1975).

Churchill, Ward and Jim Vander Wall. *The Cointelpro Papers: Documents from the FBI's Secret Wars against Dissent in the United States.* Cambridge, MA: South End Press (2002).

DHS (Department of Homeland Security). "Homeland Security Academic Advisory Council Minutes" (2013).

DHS. "FEMA 428, Primer to Design Safe School Projects in Case of Terrorist Attacks" (2012).

DHS. "Terrorist Tradecraft: Impersonation Using Stolen, Cloned or Repurposed Vehicles." https://publicintelligence.net/dhs-fbi-cloned-vehicles, April 3, (2013).

FBI (Federal Bureau of Investigation). "Former University of Tennessee Professor John Reece Roth Sentenced to 48 Months in Prison for Illegally Exporting Military Research Technical Data" (2009).

———. "Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education" (2011).

Fisk, Ralph R. "Siege at Beslan School Number One—Innocence Lost," unpublished (2014).

Ford, Dana and Ben Brumfeld. "Police: Minnesota Teen Planned School Massacre," http://www.cnn.com/2014/05/01/justice/minnesota-attack-thwarted/ (May 2, 2014).

Gallagher, Brian. "The Terrorist and WMD Threat in the Place of Worship," unpublished (2014).

Gansler, Jamie and Alice Gast. "Academics and National-Security Experts Must Work Together." *Chronicle of Higher Education* 54, no. 44, 2008: A56.

Gill, Martin. "How Offenders Say They Get around Security Measures: Why They Say It Is Easy." Dubai, UAE: ASIS Middle East 5 (2014).

Golden, Daniel. "Why the Professor Went to Prison." *Business Week* (November 1, 2012).

Goode, Erica and Serge F. Kovaleski. "Details of Tsarnaev Brothers, Boston Suspects Emerge." *New York Times,* April 19, 2013.

Hawley, Chris and Matt Apuzzo. "NYPD Infiltration of Colleges Raises Privacy Fears." Associated Press (October 11, 2011).

Hesterman, Jennifer. *The Terrorist–Criminal Nexus: An Alliance of International Drug Cartels, Organized Crime, and Terror Groups.* Boca Raton, FL: CRC Press, 2013.

"Homeland Security Academic Advisory Council Minutes." Department of Homeland Security, 2013.

IBN Live, "Terrorists Kill Man Who Gave Them Water." November 27, 2008.

Investigative Project on Terrorism. *USA v. Begolly, Emerson* (2011).

———. *State of New York v. Ferhani et Ano*. (2014a).

———. *US v. El-Khalifi* (2014b).

———. *USA v. Cromitie, James, et al*. (2014c).

———. *USA v. Fahti, El Mehdi Semlali*. (2014d).

Johnson, Bryan. "Top 10 Chilling Quotes During School Shootings." http://listverse.com/2012/05/09/top-10-chilling-quotes-during-school-shootings/ (2012).

Kephart, Janice. "Immigration and Terrorism." Center for Immigration Studies, 2005.

Leung, Rebecca. "New Video of the Beslan School Terror," edited by 48 Hours Documentary CBS News (2005).

"Lifeway Christian Resources Survey: Prayer Is Most Urgent Concern for Churches," (2005).

Lumb, David and Dominic Casciani. "Pavlo Lapshyn's 90 Days of Terror." BBC News, 2013.

Malkin, Michelle. "The Ambulances-for-Terrorists Scandal." *The Philadelphia Enquirer,* June 7, 2004.

Mayko, Michael P. "FBI: Drone-Like Toy Planes in Bomb Plot." *Connecticut Post,* April 7, 2014.

McCluskey, Brent. "Graphic CCTV Footage of Militant Attack in a Yemeni Hospital." Podcast audio. http://www.guns.com/2013/12/14/graphic- cctv-footage-militant-attack- yemeni-hospital-video/ (2013).

McDaniel, Michael C. and Cali Mortenson Ellis. "The Beslan Hostage Crisis: A Case Study for First Responders.". *Journal of Applied Security Research* 4 (2009): 21–35.

Mohr, Holbrook, Mitch Weiss, and Mike Baker. "J-1 Student Visa Abuse: Foreign Students Forced to Work in Strip Clubs, Eat on Floor." *Huffington Post,* December 10, 2010.

Mohr, Holbrook, Mitch Weiss and Mike Baker. U.S. Fails To Tackle Student Visa Abuses. AP, December 6, 2010.

"New Video of the Beslan School Terror." Edited by Leung, Rebecca, 48 Hours Documentary CBS News, 2005.

Novak, Sophie. "Should Congress Speed Up Its Push for Terrorism Protection?" *National Journal* (April 14, 2014).

Office of the Director of National Intelligence. "Annual Report to Congress on Foreign Economic Collection and Industrial Espionage." Washington, DC (2011).

Pew Research Center. "Trust in Government Nears Record Low" (2013).

Piegorsch, Walter W., Susan L. Cutter, and Frank Hardisty. "Benchmark Analysis for Quantifying Urban Vulnerability to Terrorist Incidents." *Risk Analysis* 27, no. 6 (2007): 1411–1425.

Rafalko, Frank J. *Mh/Chaos: The Cia's Campaign against the Radical New Left and the Black Panthers*. Naval Institute Press, 2011.

Schuster, Henry. "What Is Terrorism?" CNN, 2006.

Srivatsa, Naveen and Xi Zu. "Alleged Russian Spy Blends into Harvard." In *The Harvard Crimson,* 2010.

The Telegraph. "Gunmen in Pakistan Bomb Female Students' Bus Then Attack Hospital," June 15, 2013.

"Terror Operations: Case Studies in Terrorism." *TRADOC G2 Handbook No. 1* (July 25, 2007): 6–19.

Turner, Allan and Craig Hlavaty. "Thieves Take $600,000 from Lakewood Church Safe." *The Houston Chronicle,* March 12, 2014.

University of Maryland. "President's Task Force on Cybersecurity" http://www.umd.edu/datasecurity/ (2014).

US Department of Justice,. "Operation Xcellerator Press Conference." http://www.justice.gov/dea/speeches/xcellerator.pdf (2009).

———. "Affidavit, *US v. Christopher R. Mestos et al.*" 2010.

———. "Texas Resident Arrested on Charge of Attempted Use of Weapon of Mass Destruction." (February 24, 2011).

———. workpermit.com. "Foreign Students to the U.S. Skip out on J-1 Visas, Become National Criminals" http://www.workpe rmit.com/news/20 06_08_10/us/stud ent_visa_criminals.htm

WPRI Newport, Rhode Island. "Unusual Mob Partnership: Inside the Mafia Reveals Relationship with Gangs." http://www.wpri. com/dpp/target_12/insi de_mafia/Target_12_Investigat ors_Unusual_Partnership_263259 (2008).

Zuckerman, Jessica. "60 Terrorist Plots since 9/11: Continued Lessons in Domestic Counterterrorism." Heritage Foundation, 2014.

CHAPTER 6

Soft Target Threat Assessment

Malls, Sporting Events, and Recreational Venues

> I think our name, Mall of America, is attractive to people that want to hurt America.
>
> **—Maureen Bausch, executive vice president, Mall of America (Schulz et al. 2011)**

INTRODUCTION

Not only are Americans being targeted in the places in which they study, worship, and heal, but shopping and recreational venues are also now in the crosshairs of violent criminals and terrorists. These profit-taking soft targets do not want to become fortresses and typically struggle with the challenge of balancing security with a pleasant customer experience. Unfortunately, the decision to lower the security construct in exchange for customer satisfaction and loyalty presents increasing risk to those who own and operate the venues. Although terrorism insurance protects loss of assets in the event of an attack, the loss of life on a property due to an attack is disastrous from an economic standpoint, as well as politically. The terrorist's main goals are achieved: instant notoriety for the group and the cause, a ripple of fear in the community, immediate impact to a business sector, and making the government appear to be unable to protect communities and civilians.

SHOPPING MALLS

The modern shopping mall is extremely large and glitzy, hosting more than just retailers; many also have crowd-drawing attractions. For example, most new malls in the Middle East have amusement parks with small roller coasters, Ferris wheels, laser tag, bumper cars, arcades, and bowling alleys. The Mall of America in Bloomington, Minnesota, is the largest in the country; it has a seven-acre indoor theme park, theaters, and nightclubs, as well as hosting the state's aquarium. The megamall has more than 500 stores, employing close to 12,000 workers and hosting over 35 million visitors yearly, or 95,000 per day. On Black Friday 2011, the after-Thanksgiving visitor total set the mall record, with 210,000 shoppers through the doors. This business owner's dream is also a security nightmare.

Malls have a unique vulnerability: there are many entrances versus limited or controlled checkpoints, making them extremely difficult to protect. As the opening quote in the chapter alludes, the mall's name alone may entice attack. For instance the "Mall of America" and "Pentagon City" are not only venues that are soft targets with thousands of unsuspecting, vulnerable shoppers, but also could be symbolic targets. The addition of attractions in or near a mall, such as a casino, could further anger radical Islamists, as was likely the case in the Westgate Mall attack in Nairobi. A colocated aquarium, zoo, or circus could draw the ire of single-interest terrorists such as ALF, putting the mall on their radar. Indeed, intense protests against these venues happen worldwide on a regular basis by groups such as the Toronto Aquarium Resistance Alliance (TARA), Marineland Animal Defense (MAD), and Grassroots Ontario Animal Liberation (GOAL). Children's amusement park areas and daycare centers pose additional concerns as targets themselves or if the mall is attacked. These areas are typically located in a far recess of the mall and are especially vulnerable. One of the worst daycare fires in history occurred at the new, luxurious Villagio Mall in Doha, Qatar, in May 2012, killing thirteen children and four employees, as well as two firefighters who tried to rescue them.

Michael Rozin, an Israeli security expert, was formerly employed at the Mall of America as their special operations security captain and gave an informative interview about security at the facility. The mall calls its counterterrorism unit RAM, or risk assessment and mitigation. Rozin explains that, although detecting weapons is essential, assessing intent is equally if not more important. Therefore, his team was trained on behavioral recognition techniques to identify suspicious actors before they engage in a criminal or terrorist act. Rozin brought his experiences working security at the extraordinarily secure Ben-Gurion International Airport in Israel, where he learned behavioral detection and interviewing

techniques (*American Jewish World* 2011). Similarly to the discussion in Chapter 4 about HUMINT (human intelligence), human factors are extremely important in soft target situations where there are many access points such as malls and where technology, such as metal detectors and bag checks, is not available. Rozin's SIRA behavioral detection techniques are covered in Chapter 8 as an option for soft target venues that do not have the ability to control entry points.

Mall violence has dramatically increased in the last few years, with violent fights, shootings, and even bombings. On December 26, 2011, the Mall of America was the scene of multiple violent fights with over 200 youth involved. An Internet rumor about the presence of two popular rappers at the mall brought thousands of teenagers, who became enraged when they found no rappers or concert. This type of "mob violence" is on the rise in the United States and of concern in large venues. In 2011, in a racially motivated attack, a mob of fifty to one hundred African American teenagers attacked white patrons outside the fairgrounds at the Wisconsin State Fair. "Flash mob" attacks are fueled by the use of social media and have occurred in several US cities—Los Angeles, Chicago, Cleveland, Washington, DC, and Milwaukee. This type of spontaneous violence is difficult to detect and prevent; however, the recent terrorist attack against the Westgate Mall in Nairobi, Kenya, showed sophisticated planning and methodical execution, raising the bar for mall security officials worldwide.

Case Study: The Nairobi Mall Attack

Saturday, September 21, 2013, was Kenya's annual International Day of Peace. However, the day was anything but peaceful; at noon, armed militants affiliated with the Somali terrorist group al-Shabaab stormed the Westgate Mall in Nairobi, Kenya. Over the next four days, at least sixty-seven people died, 175 were injured, and the mall was destroyed. Reports at the time were disjointed and confusing and after months of investigation by US, British, and Israeli experts, there is still little clarity about exactly what transpired, who was involved, or how the Kenyan security forces' response may have exacerbated the problem. However, the successful soft target attack provides insight to security experts and first responders regarding this new page in the terrorists' playbook.

THE ATTACK

The upscale Westgate Mall, owned by an Israeli businessman, sits across a park from the US and Canadian embassies and is frequented by Westerners and affluent Kenyans, making it a lucrative target. Even after a wave of bombings throughout Kenya in 2012 at the hands of al-Hijra, an al-Shabaab-affiliated group, security

measures at the mall were described as cursory. Confidential documents accessed by the *Sunday Telegraph* newspaper showed the United Nations had been warned, in the previous month, that the threat of an "attempted large-scale attack" in Kenya was "elevated" (Pflanz and Alexander 2013). One week before the attack, Kenyan police claimed to have disrupted a major attack in its final stages of planning after arresting two people with suicide vests packed with ball bearings, grenades, and AK-47 assault rifles. A manhunt was also launched for eight more suspects (Pflanz and Alexander 2013). After the incident, Nairobi senator Mike Sonko claimed that he had warned the security services of a possible attack against the mall three months previously (*Jambo News* 2013).

The attack commenced when gunmen entered the mall and began shooting and throwing grenades. Initial reports of fifteen gunmen simultaneously entering the building from the main entrance, the rooftop parking lot, and a ramp into the basement (BBC 2013a) were disproven after reviewing CCTV footage. It appears there were likely only four to six gunmen, most of whom entered through the main entrance and then split into teams (Pflanz 2014). They carried hand grenades, AK-47 assault rifles, and ordinary munitions. Panic ensued as unsuspecting shoppers tried to flee or take cover. The initial attack was ruthless, including the killing of children who were attending a cooking competition in the parking lot. According to survivors, the attackers attempted to separate Muslims and non-Muslims and allowed most Muslims to leave unharmed. One woman declared to the attackers that she was a Muslim; however, she was shot for not being dressed conservatively enough. Hostages were gathered and held in the cinema and casino on the second floor and in the basement. The situation was extremely complex, with responding law enforcement units likely unaware of the severity of the situation or the sophistication of the actors.

Despite the first calls for help, the police did not arrive on scene until 12:30 p.m. Thirty minutes later, they entered the mall to attempt rescue operations for the unknown number of people trapped inside. Kenyan Defense Forces (KDF) military personnel arrived at 3:00 p.m. and also entered the mall, engaging the shooters. The transition of command authority at the scene from police operations to military was poorly coordinated; the police later asserted that while helping people escape, they were mistaken for the attackers and fired upon by the military (BBC Africa 2013b). The police and military were using different radio frequencies, neither had mall blueprints, and the Kenyan military scrambled to fly their best-trained soldiers back from Somalia (Kulish, Gettleman, and Kron 2013). CCTV footage shows Kenyan security forces abandoning the search for the shooters and, instead, looting stores within hours of the siege. A jewelry store was emptied, and security forces looted watch and clothing shops, grabbed cash from tills and ATMs, and tried to shoot their way into a casino safe. At about

10:30 p.m., footage shows four attackers holed up in an office, one of them injured, while security forces stroll around the mall with bags full of merchandise and cash (Dixon 2013).

By Sunday, over 1,000 people had been rescued from the mall, but government forces did not have control, and gunfire continued throughout the day. The death toll was up to fifty-nine and the attackers were still loose in the mall. Israeli commandos and specialized police officers arrived, along with American-supplied night vision goggles for the Kenyan forces. On Monday the government launched another offensive. There were loud explosions and sounds of gunfire, and smoke began to pour out of the building as the rear of the building collapsed; the death toll was up to sixty-two and it was believed there were more hostages inside. On Tuesday, the police declared the operation over, although there were still reports of sporadic gunfire as they cleared the mall. The final toll was at least sixty-seven people dead, including six security personnel and several terrorists who were in the rear of the shopping center when it collapsed. Some remains were burned beyond recognition and not capable of yielding DNA evidence; authorities believe the death count could have been as high as ninety-four (Butime 2014).

THE PLANNING

The attackers rented a small shop in the mall to gain access to otherwise prohibited areas such as storage rooms and service elevators. This also would have given them access before and after shopping hours, and they used this time to pre-position weapons and ammunition in a ventilation shaft (BBC 2013a; BBC Africa 2013b). Their presence in the mall provided opportunity to assess which areas would yield the highest casualties, and whether there were scheduled events to target, such as the children's cook-off outside the grocery store.

Western investigators from the United Kingdom, the United States, and Israel were called to help with the investigation. At one point the FBI had over eighty investigators on scene, including members of the Evidence Response Team (ERT), who helped process the scene (FBI 2014). Despite initial reports of fifteen heavily armed attackers, investigators all concluded the attack was probably carried out by a group of four to six people with only a basic plan and light weapons, grenades to gain entry to the mall, and a few AK-47s. Kenyan officials disagree, insisting that a larger force was involved in a detailed, intricate plan. A team of four to six gunmen thwarting Kenyan government control for four days makes the government look ineffectual and ill prepared, especially given the known threats against Kenya. Therefore, it is easy to see why officials in Nairobi failed to embrace the investigative reports.

There is also confusion over the status of the attackers. Although it is possible some of the attackers may have put down weapons

and left with the fleeing customers, there is no evidence to prove this theory. To add further confusion, after reviewing thousands of hours of CCTV footage, investigators from the New York Police Department said there is no evidence the militants were in the mall after the first day and they all most likely escaped in the confusion (New York City Police Department 2013). The FBI disagrees with this assessment, with their Nairobi LEGAT stating:

> We believe, as do the Kenyan authorities, that the four gunmen inside the mall were killed. Our ERT made significant finds, and there is no evidence that any of the attackers escaped from the area where they made their last stand. Three sets of remains were found. Also, the Kenyans were on the scene that first day and set up a very secure crime scene perimeter, making an escape unlikely. Additionally, had the attackers escaped, it would have been publicly celebrated and exploited for propaganda purposes by al-Shabaab. That hasn't happened (FBI 2014).

Months after the attack, precious little information has been added to the initial investigations and few security forces have been held accountable for their ineffective and even deplorable behavior at the scene. There are four men on trial in Nairobi for aiding the attackers; all deny the charges (Pflanz 2014). Pseudonyms were released by Kenyan authorities less than a month after the attacks; however, a *New York Times* article in January 2014 listed what are believed to be the men's given names, including Hassan Abdi Dhuhulow, a Somali-born Norwegian national (BBC 2013a). Al-Shabaab claimed three Americans were involved in the Westgate Mall attack, naming Ahmed Mohamed Isse of St. Paul, Minnesota; Abdifatah Osman Keenadiid of Minneapolis, Minnesota; and Gen Mustafe Noorudiin of Kansas City, Missouri, via their Twitter account, @HSM_Press (http://jihadology.net/2013/09/21/new-statement-from-%E1%B8%A5arakat-al-shabab-al-mujahidin-claiming-responsibility-for-the-westgate-mall-attack-in-nairobi/). Al-Shabaab's claims have not been confirmed by American law enforcement. In addition, additional Twitter accounts claiming to be al-Shabaab–run have suggested that other Americans were also involved.

The threat in Kenya has not subsided, and US citizens are cautioned by the State Department regarding travel to the country and the threat of attacks against soft targets and kidnapping. For example, on March 17, 2014, a SUV packed with 350 pounds of explosives was found in the port of Mombasa and there may be two additional vehicles at large (Pflanz 2014). The FBI assessment is that attacks in Kenya will continue to be al-Shabaab's primary external focus.

(Source: Kinzer (2014). Ms. Kinzer is a Reserve Air Force intelligence officer and senior intelligence consultant at Patch Plus Consulting.)

Other Significant Mall Attacks

Hamas has also started planning attacks against shopping malls. Shin Bet, Israel's intelligence agency, foiled a bomb attack plotted by Hamas timed for the High Holy Days in September 2013. Two men who were employed as maintenance workers at the upscale Mamilla Mall were planning to smuggle the bomb into the shopping center and to hide it in a closet. Their handlers ordered them to plant the bomb in a restaurant, store, or trash can and to cover it with wrapping paper, in order to make it look like a gift in preparation for the upcoming Jewish holidays, and to detonate it when the mall would be packed with shoppers. One scenario included wrapping the device in a box of chocolates and placing it in a garbage can, according to the indictment (Lappin and Bob 2013). The Irish Republican Army (IRA) has also used targeted shopping areas; on the morning of June 15, 1996, a cargo van filled with 3,300 pounds of explosives exploded in the middle of a busy shopping center in Manchester, England, injuring over 200 people. England was hosting the 1996 European Football Championship that year, and a match between German and Russian soccer teams was scheduled for the next day in Manchester's stadium.

Terrorist Threats Against US Malls

The United States has 800 shopping malls and Allied Barton Security Services is one of the largest suppliers of shopping mall security personnel, with some 12,000 officers. Their assessment on the possibility of a mall attack in the United States is that it can happen, and we need to prepare (Bradley 2013). In fact, several plots have already been intercepted by law enforcement since 9/11. Nuradin M. Abdi, a Somali immigrant living in Columbus, Ohio, was arrested in November 2003 and charged in a plot to bomb a local shopping mall and shoot the evacuating shoppers. Abdi traveled to Ethiopia purposely to receive training at an Islamist camp in construction of explosives for his operation (Investigative Project on Terrorism: *US v. Nuradin Abdi* 2014b). Abdi recently finished his ten-year term in federal prison and was deported to Ethopia.

Derrick Shareef was arrested in December 2006 on charges he planned to set off hand grenades in a shopping mall outside Chicago. Shareef acted alone and was arrested after meeting with an undercover agent. FBI reports indicated the mall was one of several potential targets, including courthouses, city halls, and government facilities. Shareef, however, settled on attacking a mall in the days immediately preceding Christmas because he believed it would cause the greatest amount of chaos and damage (Investigative Project on Terrorism *US v. Shareef*

2004). Shareef was sentenced to thirty-five years in prison without the possibility of parole.

Tarek Mehanna, previously indicted for lying to the FBI about the location of terrorist suspect Daniel Maldonado, was arrested on October 21, 2009, on allegations of conspiracy to kill two US politicians, American troops in Iraq, and civilians in local shopping malls (Investigative Project on Terrorism: *US v. Mehanna* 2014a). He was sentenced to eighteen years in jail. His coconspirator, Ahmad Abousamra, a former Boston resident who fled to his home country of Syria, is on the FBI's most wanted list for attempting to obtain military training in Pakistan and Yemen for the purpose of killing American soldiers overseas.

US malls have also been the scene of several attacks involving lone gunmen with no apparent motive, other than homicidal or suicidal intentions. On January 26, 2014, a suicidal nineteen-year-old man, Darion Marcus Aguilar, went to his favorite store, popular with skateboarders, and shot two employees and then himself at a mall in Columbia, Maryland. He also carried two makeshift bombs in his backpack that had been cobbled together with fireworks. In other random mall attacks, a twenty-two-year-old man killed two people and then himself at a mall near Portland, Oregon, in December 2012; a nineteen-year-old man killed eight people and then himself at an Omaha, Nebraska, mall in December 2007; and an eighteen-year-old man killed five people before he was killed by police at a mall in Salt Lake City, Utah, in February 2007. Malls seem to be irresistible to violent actors who want to enter the scene without being challenged and kill a maximum amount of people in the shortest period of time. Typically, they commit suicide or are killed by law enforcement; therefore, it is difficult to gather enough forensic information to profile mall attackers.

Following the Nairobi mall attack and other incidents, the FBI and Department of Homeland Security stepped up exercises at major malls in the United States as part of the Complex Mall Attack preparedness initiative established in late 2013 to promote preparedness and strengthen public/private partnerships. Exercises were held at malls in at least twelve states in 2014 with many more planned. Typically, shoppers have departed the stores and cleared the parking lots; however, the exercises include actors fronting challenges to law enforcement that would be present during busy shopping hours.

Vulnerable Open Air Marketplaces

As the center of economy for poor villages and towns, open-air marketplaces are a soft target routinely singled out in war-torn countries. The open-air market is an attractive target because overwhelming firepower

and planning are not necessary to cause mass casualties. For example, on February 5, 1994, during the Bosnian war, a 120 millimeter mortar shell fired by Serbian forces landed in the Markale marketplace in Sarajevo during the busy lunch hour. UN observers reported that l68 people were killed and 144 more were wounded. These types of attacks against innocent civilians as they go about their daily routine can even change the course of a war. Markale was struck eighteen months later, on August 28, 1995, again during lunch hour. This time, Bosnian forces fired five mortar shells, killing forty-three people and wounding seventy-five others. The event pulled an angry NATO into the conflict, and its punishing air strikes against Bosnian Serb forces brought them to the table for the Dayton Peace Accords and a negotiated peace.

Hamas and the Popular Front for the Liberation of Palestine (PFLP) routinely target open-air markets in Israel. A PFLP-led suicide attack against the Netanya produce market on May 19, 2002, killed three people and injured fifty-six. The perpetrator was dressed as an Israeli Defense Forces soldier and easily accessed the market. The entrance was selected for the attack because it historically had a bottleneck of customers and would yield the greatest number of casualties. Hamas struck the Mahane Yehuda Market on July 30, 1997, with two consecutive suicide bombings. The market is Jerusalem's main open-air fruit and vegetable market. Sixteen people were killed in the attack and 178 were injured.

We must consider the vulnerability of open-air markets in our country; for instance, farmers' markets, flea markets, and similar venues are popular on weekend days in large US cities, and they, too, are completely unprotected. As in enclosed malls, detecting bad actors and their weaponry is difficult; therefore, deterrence, mitigation, and response are critical to contain the threat.

SPORTS VENUES

Large sporting events are of interest to terrorists, and this vulnerable soft target serves two of their needs. First of all, there is a crowd of unsuspecting, vulnerable people and, second, there is the added benefit of live television coverage with the amplifying effect of terrorized viewers.

Stadiums and Arenas in the Crosshairs

Over 1,300 professional sport stadiums and arenas in the United States are used for a variety of events from school graduations to concerts, political events, and evacuation and sheltering locations in natural or national emergencies. As such, the Department of Homeland Security (DHS) has

identified sport stadiums/arenas as critical infrastructure/key resource (CI/KR) key assets. However, as with all soft target locations, the government relies on the venue owners and operators to secure their properties and users properly. College stadiums have the most vulnerability, as they rely on part-time and seasonal help to man events, and background screening is limited due to expense. Dr. Stacey Hall, an expert on spectator sports safety and security, has written several outstanding articles and books on the topic, worth review by all who own, operate, or secure these venues. According to Dr. Hall (2010), college stadium vulnerabilities include:

- Lack of emergency and evacuation plans specific to sport venue
- Inadequate searching of venue prior to event
- Inadequate searches of fans and belongings
- Improperly secured concessions
- Dangerous chemicals stored inside the sport venue
- No accountability for vendors and their vehicles
- Inadequate staff training in security awareness and response to WMD [weapons of mass destruction] attacks

Football stadiums are high on al-Qaeda's list of targets. The *Encyclopedia of Afghan Jihad* (2004), found in the London residence of Islamic cleric Sheikh Abu Hamza al-Masri, proposed football stadiums as possible terrorist attack sites. In July 2002, the FBI issued an alert warning that suspects with links to al-Qaeda affiliates were downloading stadium images from www.worldstadiums.com, including the Edward Jones Dome in St. Louis and the RCA Dome in Indianapolis (Grace 2002). In response to these and other threats, DHS developed an extensive national planning scenarios document to cover possible terrorist attacks specifically aimed at stadiums. The 2005 document specifically addressed the potential of a biological attack on a sports arena, stating that the spreading of pneumonic plague in the bathrooms would potentially kill 2,500 people. DHS's 2006 planning scenarios included a light aircraft spraying a chemical agent into a packed college football stadium, contaminating the stadium and generating a downwind vapor hazard (DHS 2006).

The only good news is that, unlike malls, entrance points to most sporting and recreating venues can be limited, bags checked, and behavior assessed. However, the cost to secure a stadium of 75,000 people or an Olympic venue is exorbitant, especially if protecting against an unknown threat. For example, in response to threats against its games, the NFL instituted mandatory pat-downs at entrances, upsetting the venues and teams, which had to pay extra for security and handle irate fans. US taxpayers were outraged at the $300 million price tag for the 2002 Winter Olympics in Utah, yet the 2014 Sochi Olympics cost $50 billion, including extreme security measures to protect from terrorist attacks.

As an international event on the world stage, the Olympics have always been a target for nefarious groups and actors. The first major terrorist attack against a sporting event was at the 1972 Munich Games, when the Palestinian terrorist group Black September took the Israeli national team hostage, eventually killing eleven athletes and coaches and one West German police officer. The world was transfixed on the event, as the kidnappers and their hostages could be seen on television through their hotel windows. German officials devised a sound rescue plan, Operation Sunshine; unfortunately, members of the International Olympic Committee were interviewed on television and gave the details. Unbeknownst to them, the terrorists were watching and learned of the plan. After more failed negotiations, a new rescue strategy was developed involving escape helicopters, with snipers targeting terrorists as they walked across the airfield with the hostages. However, the number of terrorists and their firepower were underestimated; the snipers were unable to gain control of the situation, and all of the athletes were killed in the rescue attempt.

The Olympic scene was quiet until Eric Robert Rudolph, a former US Army soldier and member of Christian Identity (a white nationalist group), attacked the 1996 Atlanta Games. At 1:20 a.m. on July 27, 1996, a bomb was detonated in Centennial Olympic Park, an entertainment and vendor area. Two people died and over a hundred were injured in the blast. According to Rudolph, in a riveting *Sports Illustrated* oral history of the bombing, the attack was meant to shut the Games down, not kill people:

> The plan was to clear the park, and hopefully after clearing the park and the explosion, this would create a state of instability in Atlanta, potentially shut the Games down or at least eat into the profits that the Games were going to make. The idea was to use them as warning devices, not to target people…In retrospect, it was a poor decision. (Zaccardi 2012)

After placing the bomb, which had a 55-minute timer, Rudolph called in two bomb threats to 911, anticipating the park would be cleared. As he watched from a distance, security officers inspected the bag and determined it was a bomb. Much to his surprise, people were still milling around the area when the device detonated: the bomb threat information was never transmitted to the scene. As Rudolph left the park, he detonated four unexploded devices in a trash can outside the park instead of planting them. Unfortunately, the security guard who originally noticed the suspicious bag containing the bomb, Richard Jewell, was named as the prime suspect while Rudolph slipped out of Atlanta. After seven years on the run and bombings at abortion clinics and a

lesbian bar, Rudolph was caught by a rookie police officer in 2003 while scavenging food from a dumpster; he is currently serving four life terms at the supermax prison in Colorado. The only attack he ever apologized for was the one against the Olympics.

The Basque separatist group ETA targeted the 2002 European Champions Soccer League final in Madrid, Spain. On May 1, 2002, a car bomb exploded near Santiago Bernabeu stadium hours before the game, and a second car bomb exploded a half hour later about one mile away. Seventeen people were injured in the attacks. However, in a show of defiance to the terrorist group, officials went ahead with the game with 75,000 fans in attendance. Also, the Boston Marathon was not the first running race targeted by terrorists. On April 6, 2008, a suicide bomber detonated a device at the start of a Sri Lankan marathon, killing fifteen people and injuring a hundred. The terrorist group Liberation Tigers of Tamil Eelam (LTTE) took responsibility for the attack (*New York Times* 2008).

There have been several sporting event threats or attacks in the United States. In June 2003, a bomb threat was made against Continental Airlines Arena during game 5 of the NBA finals, and responding police found ten cars on fire in the arena parking lot. In October 2005, an Oklahoma University student suicide bomber strapped a detonating device to his body outside the school's stadium during a football game, killing only himself. His apartment had jihadist and bomb-making material, as well as a cache of the explosive triacetone triperoxide (TATP), a favorite of al-Qaeda terrorists. In October 2006, the National Football League received an uncorroborated threat indicating the use of radiological "dirty bombs" against seven National Football League stadiums.

Finally, in the worst attack against a sporting venue in the United States, the Boston Marathon bombings on April 15, 2013, were carried out by brothers Tamerlan and Dzhokhar Tsarnaev, naturalized US citizens of Chechen descent. The attack killed three people, and wounded more than two hundred. Tamerlan was clearly the ringleader—a vicious killer who was posthumously implicated in a prior unsolved triple homicide of his best friend and two others in Boston. At some point, he was (at the very least) communicating with and inspired by radical Islamists. The brothers used an edition of al-Qaeda in the Arabian Peninsula's *Inspire* magazine to construct the pressure cooker bombs, which, interestingly, are used in many Chechen rebel attacks. However, in a show of psychological resiliency, the city hosted a marathon a few weeks later for those unable to complete the main event. In April 2014, Boston held a full-up marathon event with thousands of security officers and the event itself went off without incident. However, a week before, a man dressed in black, screaming "Boston strong," walked down the middle of Boylston Street with two backpacks containing rice cookers; the bags

were detonated by law enforcement. Although not a terrorism-related event, it rattled the nerves in the still healing city.

Other sporting venues have been targeted by the al-Qaeda splinter group, al-Shabaab, in both Somalia and Uganda. The Mexican cartels are particularly cruel, targeting children's soccer matches and sports-themed birthday parties. So the concept of sporting events as targets is not new and is being leveraged by everyone from petty criminals to major cartels and terrorist organizations.

Exploring Russia's security laydown for the 2014 Sochi Olympics provides the framework for discussion regarding the delicate balance between security, venue aesthetics, and comfort for attendees. Not only lives are at stake, but also world opinion of the host's ability to secure itself, athletes, and visitors from attack. This pressure to secure the vast venue led to heavy-handed security decisions and scrutiny, as well as exorbitant cost.

Case Study: Putin's Ring of Steel—How the Russian Federation Constructed the Most Extensive and Controversial Security System in Olympic History

In a January 2014 interview, President Vladimir Putin asserted that, "[i]f we allow ourselves to be weak, feel weak, let our fear to be seen, by doing that we'll assist those terrorists in achieving their goals" (Radia 2014). The 2014 Winter Olympics in Sochi, Russia, was historic because, for the first time, the global discussion was more focused on the escalating potential of terrorist activity against unprotected "soft" targets and the requisite security for the Games' venues rather than on the athletic competitions. With serious threats of terrorist attacks shrouding the Games, the Russian Olympic Committee generated the most sophisticated and extensive security regime in history. From deploying thousands of troops to positioning hundreds of antiaircraft missiles and implementing a pervasive surveillance system, the security at the Sochi Olympic Games was unprecedented in depth and extent. However, despite these defensive measures and Russian assurances, the world nervously speculated as to whether the Games in Sochi would be safe. Agitated by statements from terrorist leaders that they were explicitly targeting the Olympics, and suicide bombings occurring only months before the Games, world leaders, Russian citizenry, Olympic athletes, and international tourists feared that the advisories, precautions, and implemented security could not protect against potential terrorist attacks. Yet, despite the numerous threats and all of the concerns, the 2014 Winter Olympic Games in Sochi were not attacked. President Putin accomplished his goal of protecting the Games, maintaining his reputation, and promoting Russia as a powerful and impenetrable global entity. But, what was the ultimate price for Russia's Olympic success?

THE VENUE

The warmest place in Russia, and a common vacation spot for natives during the long winter, Sochi was a seemingly strange location to host the 2014 Winter Olympics. However, Sochi is a favorite locale of President Putin, who owns a personal retreat in the resort city. Throughout the history of the former Soviet Union, Sochi offered peace and quiet to many of the politically elite, including Joseph Stalin, whose former dacha (vacation home) can still be visited by tourists today. Despite the weather and the Soviet legacy in Sochi, the most surprising aspect of the city's selection was its close proximity to the volatile region of the northern Caucasus. Situated in the southwestern-most corner of Russia, nestled near the Black Sea, Sochi is separated only by the Caucasus Mountains from a hotbed of Islamic militant groups—deeply embedded, actively engaged in terror attacks, and passionately intent on attacking Putin's Russia. Sochi is just 300 miles from Chechnya and only 185 miles from Kabardino-Balkaria, site of more than sixty-nine attacks in 2013. Unquestionably, the host city of the 2014 Winter Olympics was located on the edge of a war zone.

The long and historic conflict in the northern Caucasus dates back to 1817, when Russian forces invaded the Persian-controlled region and sparked a war with the local tribes. After nearly 50 years of fighting and more than 290,000 deaths, Russia captured the opposition leader and annexed the Caucasus. Relations were further antagonized during Joseph Stalin's reign in the Soviet Union. Relying on accusations of collaboration with Nazi Germany, Stalin deported the entire Chechen population and the majority of the Ingush population to Siberia and Central Asia. The historical and cultural clash between Russia and the northern Caucasus culminated in the First and Second Chechen War during the 1990s, which took over 150,000 lives. Today, almost 200 years after the first spark of violence in 1817, relations between the Kremlin and the northern Caucasus continue to be strained and the region remains volatile.

The violence and cultural tension associated with the northern Caucasus is predominantly embedded in the republics of Dagestan, Chechnya, and Ingushetia. The North Caucasus Federal District, with a population of approximately ten million, is the smallest of Russia's eight federal districts. However, it is the most diverse district, with approximately forty ethnic groups, and the only district in which ethnic Russians are actually in the minority. Unlike the rest of the Russian Federation, Sunni Islam is the dominant religion in the northern Caucasus, with most practicing Sufism, or mystical Islam. In 2005, a group of Sunni Islam extremists in this region ignited an uprising against the Russian Federation in an effort to spurn Russian rule and establish an independent Islamic state.

The Islamist insurgency's umbrella group, known as the Caucasus Emirate or Imarat Kavkaz, imposes its religious tenets

through various acts of terrorism, including suicide bombings and army ambushes. Its mission to establish an Islamic caliphate is led by Chechen warlord Doku Umarov, whose first attack was the 2010 suicide bombing in the Moscow metro, killing thirty-nine people. He also claimed responsibility for the 2011 suicide attack at Russia's Domodedovo International Airport that killed thirty-five. Numerous other terrorist acts against soft targets have recently been perpetrated throughout Russia under the Caucasus emirate banner. In October 2013, a female suicide bomber from Dagestan killed six people and injured over thirty others on a passenger bus in the Russian city of Volgograd. Two months later, another Dagestani female terrorist attacked the same city, killing sixteen people at a local train station.

The Volgograd terrorist attacks, which occurred a mere six weeks before the 2014 Winter Olympics, caused global concern and speculation about Russia's ability to stem the increasing threats of similar attacks to soft targets surrounding the Olympic Games. These concerns were not unfounded. In July 2013, Umarov summoned his Islamist followers to make the Sochi 2014 Olympics a target of extremist activity, claiming that these "Satanic Games" were being held on the "bones of our ancestors," alluding to the fact that Sochi was the last stand for Muslims who were slaughtered and buried there during the Russian–Circassian war that ended in 1864 (*Moscow Times* 2013). Some historians agreed, stating that Russia's hosting the Olympic Games at Sochi was akin to Germany hosting games at Auschwitz (Somra and Watson 2014). So Putin's choice of Sochi was not only based on personal preference, but also incited the Chechens and brought forth memories of genocide that wiped out a generation of Russian Muslims. Media outlets around the world discussed the blatant threats of terror and ruminated over whether Russian security at the Winter Olympics would be sufficient to protect the city, the citizens, the coaches and athletes, and the tourists. The issue of security soon dominated worldwide media discussions regarding the 2014 Winter Olympics in Sochi.

THE PLAN

In response to the blatant terrorist threats and the increasingly negative media coverage of Russia's security, the Sochi Olympic Committee and President Putin implemented a public relations scheme to generate a positive perception of the 2014 Winter Olympic Games. The chief Sochi organizer, Dmitry Chernyshenko, confidently proclaimed that Sochi was the "most secure venue on the planet" (Wilson 2014). President Putin adamantly affirmed that the Sochi Games would showcase the greatness of the Russian Federation and guaranteed that "our job—needless to say, the job of the Olympics host—is to ensure security of the participants in the Olympics and visitors to this festival of sports and we will do whatever it takes" (Radia 2014).

To the Russian president and the Russian Federation, the Games were indicative of much more than just the ability to host a sporting event. More than 30 years after Moscow hosted the controversial 1980 Olympic Games, the 2014 Winter Olympics in Sochi were intended as an exposition of Russia's greatness. President Putin articulated the significance of the Sochi games stating:

> [F]ollowing the collapse of the USSR, following hard and, let's put it bluntly, blood-soaked developments in the Caucasus, the overall state society was depressing and pessimistic. We need to cheer up, we need to understand and feel that we are capable of pulling off major, large-scale projects and do so on schedule and with good quality. (Radia 2014)

As a result of the significance that he placed on the Olympic Games, the sporting event soon earned the moniker of "Putin's Games." Achieving Putin's goal and protecting his reputation came at a price tag of $50 billion, more than what was spent on all previous winter games combined. The exorbitant cost overrun of the Sochi Games is widely attributed to Russia's continued political corruption and construction-industry fraud, and one construction worker openly complained about the $50 million bribe paid to a Kremlin official to secure work at Sochi.

Kremlin officials described the impenetrable fortress of security around the Games as Putin's "ring of steel." The architect of this "ring of steel" was the appointed chairman of security for the Sochi Games, Oleg Syromolotov. Syromolotov serves as the deputy director of Russia's Federal Security Service (FSB) with particular expertise in counterintelligence. Central to the security laydown was the most extensive, sophisticated, and controversial surveillance system in operation (Matthews 2014). The 2014 Olympics became a monumental experiment for comprehensive and invasive surveillance, making Sochi the most heavily policed environment in history (Matthews 2014).

At the core of the operation was a sophisticated technical platform, the system of operative-investigative measures (SORM), which, by all accounts, makes the US National Security Agency's controversial PRISM system look elementary. First developed in the 1980s by the Soviet KGB, SORM is a nationwide electronic interception and monitoring program that authorizes numerous Russian agencies to intercept all electronic transmissions legally. The latest version, SORM-3, has been described as, "a giant vacuum cleaner which scoops all electronic communication from all users all the time" (Matthews 2014). Designed to search metadata and content, SORM-3 intercepts, collects, examines, and stores all information and communications (e.g., e-mails, social networks, phone calls) from electronic devices, storing them for future use.

The breadth of FSB's authority and SORM-3's technical ability to gather and analyze information by reading and listening to electronic communications far surpasses the capabilities of the National Security Agency's PRISM system, which Edward Snowden exposed in 2013. Sochi Olympic officials worked diligently to ensure that all Internet service providers (ISPs) installed the SORM-3 devices on their networks to provide the FSB unrestricted surveillance capability of tourists, coaches, athletes, and journalists. The Olympic Committee justified this unbridled surveillance as necessary to protect against terrorism. Furthermore, ISPs that did not have the system installed were fined by the FSB.

In furtherance of the government's antiterrorism security scheme, Russia's leading telecom operator, Rostelecom, promised to provide the fastest Wi-Fi in Olympic history by launching an extensive 4G LTE network throughout Sochi, which was offered for free to all visitors to the Games. However, with this free, rapid Wi-Fi access, all Sochi Internet users were subject to deep packet inspection (DPI), which allowed ISP providers and other intermediaries to collect and analyze the Internet communications of millions of users simultaneously. Rostelecom required the installation of deep packet to facilitate the FSB's ability to monitor and filter all communication traffic.

The Olympic Committee's conventional security was also extensive. More than 40,000 police were on duty throughout the Games guarding the Olympic city (Figure 6.1). Two sonar systems were

FIGURE 6.1 Russian military officers on patrol in Sochi during the Olympic Games.

purchased to protect against sea-launched terror attacks and, to repel a possible air attack, there were antiballistic missile batteries around the city. Finally, with more than 4,000 surveillance cameras and closed-circuit television (CCTV) technology installed, Sochi became one of the most watched cities in the world. With cameras watching at every corner and missile defense units visible to the public, many argued that the spirit of the Sochi Games was shrouded in a blanket of extensive and intimidating security measures (Bender 2014).

At first, the Sochi security officials were reserved and uncooperative, not only about sharing details regarding the scope and magnitude of the implemented security, but also about sharing the duty of security enforcement. Over time, the relationship between the FBI and the Russian FSB improved, and a month before the Games, FBI Director James Comey announced he would send about a dozen US federal agents to the Sochi Games and even more agents to Moscow. This announcement came amidst the growing concern of terrorist attacks on "soft" targets and questions about the security of the US team and others. Cognizant of the increasing terrorism threats against soft targets, a top US counterterrorism official warned a Senate panel prior to the Games that terrorists might strike targets on the outskirts of Sochi (Madhani 2014). Much to the world's relief, the two weeks of Olympic competition were carried out successfully and without any reported breach of security.

The monetary cost to protect the games was high, but the real cost for the unparalleled security at Sochi was felt at the personal level. In and around the Sochi Olympic venues, athletes and coaches, journalists, and tourists were subjected to intrusive electronic surveillance and burdensome physical security measures. In addition to posting photos of the poor sanitary and safety conditions at Sochi via the Twitter account @SochiProblems, tourists also complained (and offered proof) that their hotel rooms and bathrooms were bugged. In angry response to questions posed by reporters regarding poor facility conditions such as the lack of hot water, Russian Deputy Prime Minister Dmitry Kozak may have slipped regarding surveillance, stating: "We have surveillance video from the hotels that shows people turn on the shower, direct the nozzle at the wall, and then leave the room for the whole day" (Sridharan 2014). The price of admission to participate in, to be a spectator of, or to report on an Olympic event was the complete surrender of one's privacy. Russia believes the cost for creating an adequate defense for "soft" targets against terrorist attacks is the complete relinquishment of personal space and private information. Perhaps for those that attended the Olympic Games in Sochi, that price was not too high.

(Source: Jorns (2014). Ms. Jorns lived and studied in Russia, and she worked at the US embassy in Moscow in the months leading up to the 2014 Olympic Games.)

PERFORMING ARTS AND RECREATION VENUES

The Kennedy Center for the Performing Arts is a beautiful facility located on the Potomac River, just two miles from the White House and the Capitol. On a typical Friday or Saturday evening, there are dignitaries and public figures in attendance, sitting in front or perhaps viewing from the president's or vice president's box, as I was fortunate to do some years back. The annual star-studded Kennedy Center Honors event is even televised live and the holiday concert is often attended by both the president and vice president. It does not take a security expert to realize this venue, which also has an underground parking garage, is a prime soft target for a bold and shocking terrorist attack.

Case Study: The Dubrovka Theater Attack

The Dubrovka Theater in Moscow is a similar venue to the Kennedy Center and was the scene of a horrific Chechen terrorist attack on October 23, 2002 (Figure 6.2). Around 9:00 that evening, during Act II of a sold-out performance, forty-one heavily armed and masked men and women drove a bus directly into the theater's main hall, firing assault rifles. Within seconds, 916 people were taken hostage, including a Russian general, while ninety people managed to flee the building or hide. The terrorists had grenades, improvised explosive devices strapped to their bodies, and they wired large bombs throughout the theater. The terrorists stated that they had no anger toward foreigners and promised to release anyone who showed a foreign passport. About 200 hostages were released, including some children, pregnant women, and foreigners. The rest were kept in the theater at all times, using the orchestra pit as a lavatory. As the situation moved into its second day, both an outsider

FIGURE 6.2 CCTV still from inside the Dubrovka Theater, Moscow.

who entered the theater to find his son and a hostage who stormed a terrorist were killed.

The mass death toll resulting from the siege actually came at the hands of the Russians themselves during a poorly executed "rescue" on the third day of the standoff. After Special Forces troops stormed the theater, President Putin ordered security forces to inject a substance into the ventilation system, an aerosol anesthetic that was possibly weaponized fentanyl or Kolokol-1, an artificial, powerful, opium-like substance. Instead of merely going to sleep as the government hoped, people suffocated as their tongues relapsed in their mouths, blocking the airway passage. Medical personnel at the scene did not have the proper antidote, and in all, 130 hostages died. In a stunning admission, Moscow's health committee chairman announced that all but one of the hostages killed in the raid had died from the gas (BBC News 2002). Those who survived the attack face a lifetime of health-related issues. The terrorists leveraged mass media to broadcast the event live to the world and allowed those in the theater to use their cell phones to call family and friends. Prior to the theater attack, the Chechens were merely fringe actors, an irritant to the Russian government. However, the siege brought Moscow to its knees as it negotiated with the terrorists and the world critically judged the government's handling of the crisis. The Chechen Rebels were now a formidible terrorist organization.

Since the Dubrovka Theater attack, other theater and concert events have been targeted by terrorist groups or had to increase security due to a general rise in the threat level. Recent, substantiated terrorist threats have been made against overseas venues hosting US singers such as Madonna (St. Petersburg and Moscow, 2012), Lady Gaga (Indonesia, 2013), and Aerosmith (Indonesia, 2013). On July 3, 2013, New York City canceled a Jay-Z concert due to security concerns that included possibility of a terrorist attack. Also, intercepted al-Qaeda communications indicated the Lollapalooza music event in Chicago was targeted in 2013.

Large outdoor music festivals are also a concern. For instance, the Bonnaroo Music and Arts Festival in Tennessee is now ranked near the top of the list of potential terrorist soft targets in the state. With over 80,000 music fans packed into a rural area and thousands of vehicles, the event is a security challenge. One solution has been to increase the number of undercover officers working the crowd.

Amusement parks present yet another security concern and challenge. Since 9/11, Disney properties have been assessed by terrorist groups as potential targets or have assumed an increased security posture due to an overall increase in threat levels in the United States. Certainly, amusement parks are vulnerable to attack, and many have increased bag inspection and limitation of items that may be brought into the park. Because

bringing weapons through the gate is unlikely, the threat of chemical or biological attack might be more probable. Also, similarly to the Westgate Mall attack, the insider threat to an amusement park is a distinct possibility. Park employees are able to carry out reconnaissance on possible targets and pre-position materials needed for an attack. Therefore, screening of potential workers and vigilance concerning their activities is paramount to preventing a deadly attack from within.

TOURIST SITES: A VULNERABLE TARGET

Attacks on tourists are also a tactic in the al-Qaeda playbook that could be used at any number of locations in the United States. On November 17, 1997, at 8:45 a.m., during peak tourist entrance into the park, six Islamist terrorists from Jihad Talaat al-Fatah, masquerading as Egyptian security forces, killed the two armed security guards and then stormed the Deir el-Bahri, an archaeological site in Luxor, Egypt. Tourists were trapped inside the ancient buildings, and the terrorists went on a rape, mutilation, and killing spree, taking sixty-two lives. The terrorists escaped the scene in a tourist bus; at a checkpoint, they scattered into the hills. Some were later found dead, having committed suicide. The tourist industry in Egypt, especially at Luxor, was deeply affected and has never fully recovered. The massacre did serve to turn Egyptian public opinion against al-Fatah and forced the government into action against the group, which later claimed that it did not carry out the attack and blamed Osama bin Laden. Several tourist sites in the United States could lend themselves to a similar attack, particularly where a few guards could be overtaken and visitors trapped and taken hostage.

These examples show that recent history is replete with examples of attacks on or threats against shopping, sports, and recreational venues by groups that threaten the United States. The next chapter explores how countries with more experience in soft target attacks, such as those in the Middle East, harden their civilian-centric facilities to deter or repel terrorist attack.

REFERENCES

"Al-Shabaab Twitter messages during the Westgate Mall Attack" http://jihadology.net/2013/09/21/new-statement-from-%E1%B8%A5arakat-al-shabab-al-mujahidin-claiming-responsibility-for-the-westgate-mall-attack-in-nairobi/ (2013).

American Jewish World. "Israeli Counters Terror at Mall of America," February 2, 2011.

BBC. "Nairobi Siege: How the Attack Happened." 2013a.
BBC Africa. "Q&A: Westgate Attack Aftermath." (October 21, 2013b).
BBC News. "Gas 'Killed Moscow Hostages.'" (October 27, 2002).
Bender, J. "Security Measures That Will Put a 'Ring of Steel' around the Sochi Olympics" (January 31, 2014).
Bradley, Bud. "State of U.S. Mall Security Post 9-11" (December 17, 2013).
Butime, Herman Rujumba. "The Lay-out of Westgate Mall and Its Significance in the Westgate Mall Attack in Kenya." *Small Wars Journal* (May 10, 2014).
DHS (Department of Homeland Security). "National Planning Scenarios" (2006).
Dixon, Robyn. "Video Shows Kenyan Soldiers Looting Besieged Mall." *Los Angeles Times,* 2013.
Encyclopedia of Afghan Jihad, 2004.
FBI. "On the Ground in Kenya—Part 2: Terror at the Westgate Mall," 2014.
Grace, Francis. "FBI Alert on Stadiums." CBS News, July 3, 2002.
Hall, Stacey. "Securing Sport Stadiums in the 21st Century: Think Security, Enhance Safety." *Journal of Homeland Security* (2010).
Investigative Project on Terrorism. "US v. Shareef, Derrick" (2004).
———. "US v. Mehanna, Tarek" (2014a).
———. "US v. Nuradin Abdi" (2014b).
Jambo News. "Nairobi Senator Mike Sonko Reveals What He Knew about Westgate Mall Terrorists," October 10, 2013.
Jorns, Eileen. "Putin's Ring of Steel: How the Russian Federation Constructed the Most Extensive and Controversial Security System in Olympic History" (2014).
Kinzer, Sarah. "The Nairobi Mall Attack" (2014).
Kulish, Nicholas, Jeffrey Gettleman, and Josh Kron. "During Siege at Kenyan Mall, Government Forces Seemed Slow to Respond." *New York Times,* October 1, 2013
Lappin, Yaakov and Yohah Jeremy Bob. "Shin Bet Foils Hamas Bomb Attack Planned for Jerusalem Mall." *Jerusalem Post,* September 2, 2013.
Madhani, Aamer. "U.S. Worried About Attacks on Soft Targets near Sochi." *USA Today,* January 29, 2014.
Matthews, Owen. "Russia Tests 'Total Surveillance' at the Sochi Olympics." *Newsweek* (February 12, 2014).
Moscow Times. "Islamist Umarov Vows 'Maximum Force' to Stop Sochi Games," July 3, 2013.
New York City Police Department. "Analysis of Al-Shabaab's Attack on the Westgate Mall in Nairobu, Kenya," 2013.
New York Times. "Suicide Bomber Kills Official and 13 Others at Sri Lanka Race," April 7, 2008.

Pflanz, Mike. "Nairobi's Westgate Mall Attack: Six Months Later, Troubling Questions Weigh Heavily." *The Christian Science Monitor,* March 21, 2014.

Pflanz, Mike and Harriet Alexander. "Nairobi Shopping Mall Attacks: Britons among Those Caught Up in Terrorist Assault." *The Telegraph,* September 21, 2013.

Radia, Kirit. "Putin: 'Can't Feel Weak' in the Face of Terror Threats to Sochi Olympics." ABC News and World Report (January 17, 2014).

Somra, Gena and Ivan Watson. "Circassians: Sochi Olympians 'Are Skiing on the Bones of Our Ancestors.'" CNN (February 18, 2014).

Sridharan, Vasudevan. "Sochi Winter Olympics 2014: Hotel Rooms and Bathrooms 'Bugged.'" *International Business Times,* February 8, 2014.

Wilson, Stephen. "Sochi Chief: City Is World's 'Most Secure Venue.'" Associated Press (January 29, 2014).

Zaccardi, Nick. "An Oral History of the Bombing That Rocked the 1996 Atlanta Games" (July 24, 2012).

Zwerdlng, Daniel, G. W. Schulz, Andrew Becker, and Margot Williams. "Under Suspicion at the Mall of America." National Public Radio (September 07, 2011).

CHAPTER 7

Hardening Tactics at Global Hotspots

We will bankrupt ourselves in the vain search for absolute security.

—Dwight D. Eisenhower

INTRODUCTION

At this point in the book, you may be feeling overwhelmed, with knowledge of the vast international and domestic terror threats against soft targets and the unique vulnerabilities at your institution or place of business. How can you possibly protect your facility and its innocent occupants from a variety of threats ranging from anthrax to a car bomb to an active shooter? The good news is that hardening best practices can be harvested from different countries and sectors and then cross-applied to our unique situations.

Perhaps the best perspective a security expert can have is from afar, as an observer with a broadened perspective. I have been fortunate to live near London twice: during a period of IRA bombing activity in the mid-1990s and, after 9/11, during al-Qaeda threats and attacks. I now reside and travel extensively in the Middle East, a region that has experienced years of repelling invaders and whose political unrest with the Arab uprising created a "nursery" for extreme Islam. I have witnessed the loss of freedom and privacy that is the slippery slope of security; however, the threat level is high and being safe is more important than parking right next to an entrance or getting through an airport security line 20 minutes sooner. Living in an Arab culture with a recent history of infiltration, unrest, and violence at the hands of our *mutual* enemy, radical Islam, has given insight into the myriad vulnerabilities we still have at home, and how much risk we assume in the name of convenience or aesthetics.

The 9/11 attacks propelled the United States into two major conflicts carrying exorbitant costs, which likely contributed to the crash of the US economic system. Thousands of young, promising lives were lost on the

battlefield, adding to the human toll of the 9/11 attack. Although the successful and tragic strike on the homeland rattled our entire country, the violence was isolated to New York City; one building in Washington, DC; and a field in western Pennsylvania. As much as the attack damaged our psyche and pride, we were back to "business as usual" in no time. Although obviously pained by the events of the day, most of America was immune to seeing the damage firsthand, or smelling the smoke that lingered in the hallways of the Pentagon for months. The attack was viewed by many as a "one off" event that could never be replicated, the attackers as "lucky" to pull it off. However, Americans questioned the government's ability to identify and communicate the threat.

In an attempt to help manage the residual fear, the Department of Homeland Security (DHS) instituted a color-coded Homeland Security Advisory System, which ultimately failed because it barely budged from yellow (elevated risk), despite multiple threats and successful attacks. In a nine-year period, orange (high) was used five times, and red (severe) was used just once, targeted only to inbound aircraft from the United Kingdom. People started ignoring the alert system, which "taught Americans to be scared, not prepared" (CNN 2011). The color-coded system replaced with the National Terrorism Advisory System, or NTAS, was meant to provide more special targeted information regarding threats, yet it has also been met with a general sense of apathy. Months have gone by without alerts despite the unraveling of plot after plot against our country. As we move farther from the attacks of 9/11 without the once-dreaded dirty bomb, chemical or biological attack, or other mass casualty event, the citizens of the United States have moved on psychologically. Even foiled plots barely get press coverage and have become routine news. Of course, security officials know that for every identified or failed plot, there could be many others in planning stages but the overarching threat is downplayed in the interest of keeping the public calm.

For example, the first domestic terror attack against the grid, the shooting of a key power substation in California in April 2013, was kept quiet from the public for almost nine months (Hesterman and Kinzer 2014). The way we have chosen to adapt to this asymmetric enemy is to become comfortable with ambiguity and silence, hoping for the best instead of searching for the "black swans." Except for security professionals, intelligence analysts, law enforcement, and first responders who lie awake at night thinking about the next attack, we have become complacent as a society regarding the threat. There are countries and regions that are better prepared and engaging in activities to protect their soft targets from physical to personal hardening, many of which we would be prudent to adapt.

SOFT TARGET HARDENING IN THE MIDDLE EAST

Security fatigue and complacency are something the Middle East knows nothing about after decades of conflict along religious and political lines. Often, the threat requires security procedures that would enrage most Westerners. For example, Ben Gurion Airport is one of the most secure in the world. The first ring of security is along the road to the airport, where your driver will stop at a checkpoint and be asked questions about you and your behavior (in Hebrew). He may be asked more questions after pulling up to the terminal. Cab drivers are part of the security fabric in Israel, as are barbers, street corner vendors, bartenders, and anyone else in contact with the public who may hear, see, or sense something out of the ordinary. Relationships between Israeli intelligence and law enforcement and their sources are strong and built over time. The bond maybe be cemented with occasional gifts and invitations to the home for dinner, activities that are illegal for law enforcement officers and their confidential informants in the United States. The hope is that, one day, the source will make a call and stop a chain of events leading to an attack.

The layers of security inside the airport are impressive, starting with a very direct, eye-to-eye interview about your visit. Every answer leads to another question—prying questions which are meant to intrude and trip you up. Under this intense pressure you will likely start stuttering and sweating, even if guilty of nothing. If you pass the interview, a sticker is placed on the luggage or ticket in a certain color and with a number. Next, you proceed to a screening area, where hand-carried luggage and checked luggage are thoroughly examined. All zipper compartments are opened and every object (including personal care items) is handled and swabbed to detect explosive material. After this intrusive search, the security screener walks you to the check-in counter, to maintain positive control of you and your bags. After check-in, it is time for the security line, which is determined based on the barcode number on the colored sticker. The first number is the key, with 1 being "no risk" to 6 indicating "high risk." In the higher risk lines, you will be subject to a very thorough pat-down, and possibly asked to undress. Once again, the carry-on luggage is unpacked and all electronic items scrutinized, including chargers. Your carry-on bags may even be taken away from you, into a separate room for inspection. USBs, DVDs, CDs, and even computer hard drives may be taken and screened in a separate room, and it is likely that your photo and possibly fingerprints will be run through multiple databases. If your computer or phone battery is dead, and you have no way of charging it to prove you can turn it on and off (sign that it is not a bomb), the electronics may not accompany you on the aircraft.

Young men traveling alone are suspicious, as they may be terrorists. Young women traveling alone are suspicious, as they may have a Palestinian boyfriend who asked them to bring something onboard the flight. Checking no luggage is suspicious; it means you may have reason to believe the plane will not be landing. Those with tattoos or piercings or who are sloppily dressed are suspicious: Agents may wonder about their activities in the country in previous days. Anyone who has visited any Arab country buys himself or herself at least an extra hour of discussions. Those with an Iranian stamp in their passport may be detained much longer. Some people are even escorted by military police directly to their seat on the plane, with no bathroom or shopping stops en route. And to think US citizens complain about the backscatter full-body scanners!

The point: there is a continuum of threat assessment and accepted mitigation tactics. The area in between determines the risk. Israel is a small country surrounded by larger ones with terrorist groups with one goal: to annihilate the Israeli nation. Naturally, their security procedures match the threat, and they are willing to forgo the privacy of travelers for security, even at the risk of repelling would-be vacationers and Holy Land pilgrims. The good news for air travelers departing from Ben Gurion Airport is there will be no hijacking, and a plane filled with innocent civilians will not be turned into a missile, as our US aircraft were on 9/11. But security comes with a price.

Life in a Compound

The Middle East has a "compound" mentality. Housing compounds are luxurious, self-contained neighborhoods, often with one thousand or more residents. Western wear, smoking, and alcohol are allowed inside the compound. Our compound has two fabulous pools, a restaurant, an ATM, a beauty salon, a small grocery store, a clubhouse, dry cleaners, a large fitness center, tennis courts, and a daycare. Houses are constructed with concrete block reinforced with steel rebar, and external and internal doors have security locks. Compounds are sealed up behind tall concrete walls with one gated entrance with several security guards, pop-up barriers, large sliding gates, and swing-up arms. Security vehicles are parked outside the compound entrance and just inside, as well. Many compounds have a skewed entrance, to prevent a vehicle (perhaps laden with a bomb or shooters) from running the gate and making it into the housing area or the clubhouse. Nearly every inch of compound property and exterior wall is covered by CCTV. The guards know both the vehicles and the occupants, and all visitors are stopped and challenged, forfeiting a form of picture identification that security holds until they

exit. Outside in the community, many businesses are set back from the road, also behind concrete walls and with gates and buzzers. Malls, shopping centers, and grocery stores have robust security inside as well as outside in the parking lot. Most countries have resisted building parking garages and underground parking decks due to security concerns, opting for large parking surfaces despite the searing heat. The security posture is truly impressive.

Interestingly, there is little to no crime in the Middle East. Living under Sharia law means that even expatriates are subjected to both punishments meted out in the Koran and given by a judge (sans jury). Third-country national workers value their jobs and do not want to risk deportation. There is basically no theft and no assault. In the city where I reside, there have been two murders in two years—not bad for a population of a few million. Of course, there is very little alcohol and no drugs, gambling, pornography, prostitution, or weapons, so many of the provocations and instruments that drive crime are removed from society. So why the "compound mentality"?

The answer is terrorism. Since 9/11, al-Qaeda groups have repeatedly struck targets in Muslim countries, lashing out at moderates in the name of extremist Islam. The Arab Spring uprising also opened the door for radical terrorist groups to step in and leverage the chaos to their benefit. Countries such as Jordan and Egypt have experienced thousands of demonstrations since 2011, ranging from a few dozen peaceful participants to more than 20,000 angry protestors. Libya has also been the scene of violent protest, as well as acts of terrorism perpetrated by al-Qaeda loyalists. The Syrian civil war is raging, with spillover into Lebanon, where Hezbollah has stepped up its strikes against soft targets. Stability in Iraq is sliding backward as al-Qaeda splinter ISIS attempts to destabilize new governments and take advantage of US and coalition withdrawal from military and security operations. Yemen is in steep decline, with AQAP battling for control of the country. Consider that the entire Arabian Peninsula could fit inside our country's borders with room to spare; spillover of violence into relatively peaceful countries is a daily threat. In the crosshairs are schools, churches, hospitals, housing compounds, and marketplaces which must be hardened against the potential threat.

The Arabian Peninsula has also been the site of terrorist activity against soft targets. Saudi Arabia was the scene of horrific attacks on luxurious Western housing compounds. On May 12, 2003, three compounds in Riyadh were attacked at night with car bombs and al-Qaeda terrorists with machine guns. In all, 39 people were killed, and over 160 wounded. Proving again that shared religion and ethnicity are not a factor to religious extremists, al-Qaeda terrorists attacked on November 8 of the same year, using a vehicle-borne explosive device against an Arab-occupied housing compound, killing at least seventeen people and

wounding 122 others. At 6:45 a.m. on May 29, 2004, seventeen terrorists from the group, "The New Jerusalem," the precursor to al-Qaeda in the Arabian Peninsula, attacked three targets in the city of Khobar: two Arab oil companies and a Western housing compound, the Oasis. During the 25-hour siege at the compound, schoolchildren were shot and killed, and Westerners were either beheaded or had their throats slit when they tried to escape at night. The terrorists took eighty-eight hostages, injuring twenty-five and killing twenty-two.

A friend and colleague, Lt. Col. Ed O'Neal (US Air Force, retired) was in the compound that day and was struck five times by ricocheting bullets as he tried to lead others to safety. As soon as he and colleague Lt. Col. James Broome realized the compound was under attack, they ran to the tallest building on the property, a tower. After barricading the front door, they worked their way to the roof, gathering four workers in the building along the way and grabbing a cooler of water. They spent the next eleven hours hiding on the roof in the searing 120° heat, each man only taking a tablespoon of water to conserve supplies. Saudi forces did not arrive at the compound for several hours, while the terrorists kicked in doors, killing Westerners and taking hostages across the compound. They were told via cell phone that it was safe to come out, so the two officers made their way down to the back door, removed the barricade, and opened the door to a hail of gunfire from the waiting terrorists. Both were shot by rounds from an AK-47, yet had to wait several more hours for rescue and transport to the hospital (Cobb 2005). Thanks to Ed's story, I now keep a supply of water on the third floor of our compound house and have thought of ways to quickly barricade the front door. Case studies of soft target attacks abroad are very instructional, not only for counterterrorism purposes but also for general safety and security practices in all businesses and homes.

The stituation in the Middle East can also change at a moment's notice and are not always along secular lines, as might be expected. When the United States was poised to engage in Syria in August of 2013, the Gulf Cooperation Council (GCC) states were split about military intervention and whether they would give support with their own money and troops, and/or host bases where Americans and allies would launch their assaults against the Assad regime. As the crisis cooled, the GCC resumed discussions about tightening the alliance. However, the good feelings from the summit did not last long; Saudi Arabia, viewed by many in the region as a sleeping giant, unexpectedly rose in March 2014, confronting Qatar about its alliance with the Muslim Brotherhood. The United Arab Emirates and Bahrain joined Saudi Arabia, with the three countries withdrawing their ambassadors from Doha. Many feared the GCC was unraveling and speculated the impact might have on oil prices and relationships with regional wildcard, Iran. Saudi Arabia threatened

a blockade on goods coming into Qatar, both on roads and the Arabian Sea. Qatar stockpiled refrigerated trucks filled with juice and other perishables, and locals braced for sanctions. The saber-rattling quieted over time, and rhetoric was reduced to the level of a "brotherly fight." The regional turbulence is why the Middle East fortifies soft targets. There are no color-coded charts or alerts; the threat is consistently high.

Schools and Christian Churches

Schools, churches, and hospitals are also secured. For example, international schools located in the Middle East typically have high walls and a low profile. The name of the school is not advertised, and no host country flags are seen from the outside. Students are transported in small buses with both a driver and another adult; the curtains are always drawn. Buses are cleared by security and then are driven into a special secure area obscured from public view, where children walk directly into the school. Students who walk to school, teachers, and visitors access the grounds through entry control points with standoff protection and are manned with at least two guards. All students and visitors pass through a metal detector. Despite its austere look from the outside, once on the property, schools are very open and lush, with gardens, fountains, and lovely buildings. Colleges have the same level of security. For example, at the Education City in Doha, Qatar, universities from the United States, including Georgetown, Cornell, MIT, and Texas A&M share a secure campus with stunning architecture and landscaping (Figure 7.1).

Some countries in the Middle East are allowing megachurches to be built for their Catholic, Anglican, and Greek Orthodox expatriate populations (Figure 7.2). One uses the model where Christian churches are grouped together on property outside the city and secured in a compound-like setting with security and limited entry points. No crosses are visible from the outside; this posture "lowers the heat" on the religious area, instead of taunting would-be religious attackers.

Hospitals in the Middle East are massive structures with plenty of standoff protection attractively disguised as grassy knolls, decorated stairs, fountains, and sculptures (Figure 7.3). The emergency room, ground zero for many terrorist attacks, is hidden and secured. Security guards are constantly patrolling the grounds and cameras capture every angle.

Hotel Security

Although hotels are not specifically covered in this book, their security practices may be applied to other institutions. As discussed in Chapter 3,

FIGURE 7.1 US universities in the secured Education City complex, Doha, Qatar.

FIGURE 7.2 Courtyard of Church City, Doha, Qatar, hosting Catholic, Anglican, and Coptic Christian churches.

international terrorists have targeted hotels repeatedly in the last fifteen years, with attacks resulting in thousands of deaths and injuries. Indeed, hotels provide many security challenges; vehicles can drive right up to the entrance and are often left unattended during check-in. Baggage is unloaded and brought directly into the lobby, where, again, it may be left for periods of time. Most facilities include restaurants and conference and special-event facilities that can greatly boost the building's population during peak use.

FIGURE 7.3 Hospital in Doha, Qatar.

Due to a recent history of attacks, hotels in the Middle East are extremely secure. In the fall of 2013, I was fortunate to spend five days on the ground (and off the radar) in Jordan. We first stayed at the Days Inn in Amman, Jordan. My security team was not too excited with this choice, because the hotel was one of three attacked in Amman by Iraqi al-Qaeda operatives on November 9, 2005. On that date, the Days Inn, Radisson SAS (now known as the Landmark), and the Grand Hyatt were simultaneously attacked by suicide bombers. In all, fifty-nine people died and one hundred fifteen were injured. At the Radisson, a husband/wife team entered a Jordanian wedding reception of nine hundred people and detonated their belts. Fortunately, the female bomber's belt did not work, keeping the casualty count lower than it might have been but killing at least thirty-eight. At the Hyatt, the lone bomber went to the hotel coffee shop and ordered an orange juice. After drinking it, he left and went to another room, donned his suicide vest, came back, and then detonated the explosive device. At the Days Inn, the suicide bomber walked into the entrance toward the bar/dining area. An alert employee noticed the man and called for security; the man left the building and detonated his vest in the street, killing three members of a Chinese delegation.

Of course the Days Inn in Amman now is a fortress. Security officers and vehicles are visible outside the facility; inside, they are undercover, but "present." No vehicles may stop in front of the hotel; the former "pull through" area is now filled with decorative concrete planters and other barricades. All property visitors enter an external building where luggage and handbags are screened for weapons and explosives. Individuals may be wanded (wands are handheld detectors), and questions are asked about country of origin and travel plans inside Jordan and/or neighboring countries. At check-in, passports must be shown and

the numbers are recorded in the registry. Yes, this type of security is inconvenient, but what better place to stay in Jordan than a hotel that was previously hit and now has blast-proof windows, standoff protection, and its own small police detachment? Any would-be attacker will certainly drive by this property in search of an easier target. Dining in the lobby—steps from the scene of the attack eight years prior—was not even the least bit nerve wracking.

Driving southwest from Amman, we were stopped at several checkpoints and asked for our passports and itinerary. The travel agency provided a copy of the itinerary and told me repeatedly not to lose it, and after showing it for the fourth time in a day's travels, I understood. The concept of internal checkpoints is hard to get used to, but in Jordan, home to millions of refugees from Syria, Lebanon, Iraq, and Egypt, it is easy to understand why they need to know who is moving about the country. The Jordanians are a warm, open people, influenced by the ancient European trade in the southern port city of Aqaba, and they love Americans. Everywhere we were greeted with handshakes and even hugs; however, we were not exempted from the security checks. Approaching our next destination, the Holiday Inn at the Dead Sea, we had a taste of resort security in the Middle East. At the nearby Red Sea, luxurious beachfront resorts have been subjected to horrific radical Islamist attacks against vacationers: in 2005 at Sharm el Sheikh, in 2006 in Dahab, and in Taba, Eliat, and Aqaba—all located at the mouth of the Red Sea where Israel, Egypt, and Jordan intersect. As a result, the Jordanian Dead Sea resorts less than 150 miles away are extremely secure. The Holiday Inn had several layers of security, and entering the property was like driving on a very secure military installation. However, as with most fortified places in the Middle East, the grounds inside were luxurious and the atmosphere extremely relaxed. Traveling in the region, I witnessed firsthand the possibilities of achieving the desired security/convenience/aesthetics balance.

Another technique of US hotels in certain Middle Eastern countries is using no signage and flying the flag of the host country at the entrance so the property more resembles an office building. I took the picture in Figure 7.4 of the property of a well-known US chain in a major Middle Eastern city; see the multiple concrete barriers in front of the hotel and the addition of blast-resistant glass. The photo was taken from the parking lot, where all guests must park and walk through a gate, clear security, and then enter the lobby. At the center is the flag of the host country. No signage appears on the building.

Of course a terrorist can find a specific hotel if that is the primary target; however, it certainly does not hurt to lower the "heat" and profile of the building for opportunists. Because most travelers nowadays book hotels online and not by line of sight, properties in major cities

FIGURE 7.4 US hotel in a Middle Eastern city.

and resorts might not be adversely affected by less signage. A few hints received from security professionals when staying in hotels in Middle East hotspots were to stay above the second floor, where blast damage would be less than on the ground floor, but not on the top floors, from which it would be difficult to evacuate. Also, I have learned the importance of asking for a room in the back of the building, away from the front lobby area, as that is typically the scene of an attack. Furthermore, it is prudent not to have a room facing an enclosed courtyard because rescue vehicles and ladders cannot access the area. As in any situation, individual preparedness when staying at high-profile hotels is important, for example, counting the doors to the stairwell so it can be found in the dark and/or thick smoke, and testing emergency stairwells to ensure that doors at the bottom are not locked. Also, travelers may want to reduce their time in public spaces; in the Mumbai attack and others, most people were killed in hotel restaurants and bars. Finally, consider staying in a smaller or boutique hotel, because these do not attract terrorists looking for high casualty counts.

Staff training is a key part of the hotel security framework. Recognizing the importance, the Department of Homeland Security produced an outstanding film in 2010 called "No Reservations: Suspicious

Behavior in Hotels" (http://www.youtube.com/watch?v=ZLCCvjJJZ4w). Going one step further, Safehotels (http://www.safehotels.se/?lang=en), a company based in Sweden, is the first global organization certifying hotel properties based on standard criteria which measures security training and equipment, crisis management response, and fire and evacuation procedures. The certification benefits property owners and travelers alike. US chains that have properties certified by Safehotels include the Courtyard by Marriott, Radisson, and Clarion Hotels.

A company in Africa has studied recent terrorist attacks on hotels and designed a new type of secure hotel. The Southern Sunshine Hotel factors the issue of terrorist attack into its design; for example, all of the rooms directly "communicate" with the outside through large openings, making escape and rescue operations easy in case of terror attacks or fire outbreak. The staircase area and the corridor access to all rooms are also open to the outside so there is no cover for terrorists to hide and conduct a siege of the building. Finally, the hotels will only have twenty-eight rooms, making them lower profile and less inviting to terrorist attack (Gichuhi 2014).

The Westerner as a Target

As a Westerner in the Middle East, I am a possible target or, at the very least, a person of interest. Because I cannot carry a gun, a knife, or even pepper spray for self-defense, I have learned to lower my own profile and deter a possible attacker. As a blonde-haired, blue-eyed American, it can be difficult to blend in even wearing a hijab head covering, but there are steps I have taken to keep from standing out. For instance, I have learned a few Arabic phrases to show a willingness to be part of the culture, instead of forcing my language on the host nation populace. I wear loose-fitting, conservative clothing, ensuring my shoulders, knees, and chest are covered, and I will often add a local accessory such as a scarf or jewelry. I pull my hair back and sometimes cover it with a scarf if shopping or driving in a mostly Arab area. I purchased a vehicle in the country, so it has Arab markings. When parking in lots, I am careful not to leave anything in the open that is Western in style or belies my nationality. I have learned how not to make eye contact or start conversations with host nation citizens unless necessary. I use cash at the local stores and give a different first name, if asked. Kidnapping is a rising threat in the region, so great care is taken not to be alone at night on the road or in a shop in the windy, chaotic souqs. Do not misunderstand—Arabs are kind, welcoming people and I enjoy their culture, being in their homes, and having them in mine. I just do not want to be the trigger for a radical Islamist in wait who is having a bad day and looking for a target.

This type of opportunist crime and terror attack has occurred at the entrance of the mosques and in shopping areas, so always best to lower the "heat" and attempt to blend in. Interestingly, some Arabs I have spoken with feel the exact same way when visiting the United States, and they attempt to lower their profile by staying in large cities and altering their traditional clothing if possible.

STATE DEPARTMENT ENGAGEMENT

> All of us want to be able to say truthfully, "I did my very best" when looking into the eyes of grieving survivors and family members.
>
> **—Ambassador Prudence Bushnell**
> **(US House of Representatives 2005)**

Prudence Bushnell made this statement in a congressional hearing on May 10, 2005. She was the ambassador to Kenya during the al-Qaeda attack on the embassy in Nairobi on August 7, 1998, and was knocked unconscious by the bomb blast and cut by flying glass. After receiving basic treatment at a nearby hotel, she oversaw rescue operations. She attended the funerals of twelve embassy staff personnel killed in the bombing, a task no government leader, school principal, or church or business leader ever wants. She was also present at memorial services for the two hundred one local nationals killed in the blast, who were also her embassy employees.

Embassies around the world were fortified in light of the twin bombings that day. At nearly the exact time the vehicle bomb exploded in Nairobi, the embassy in Dar es Salaam, Tanzania, was similarly attacked, killing eleven. However, in 2005, the State Department realized the growing threat to the families of their personnel stationed abroad, stating in a Congressional hearing:

> But as embassy and consulate compounds are fortified, US government personnel and their families living and working outside those walls draw the aim of criminals and terrorists looking for the next tier of targets. So hardening official buildings is not enough. The security of soft targets hinges on the harder tasks of building personal awareness and sustaining institutional vigilance. Adding cement to the physical plant is an easy part. Precious lives depend on strengthening protections for America's human capital abroad. (US House of Representatives 2005)

The State Department now has a budget to protect the family members of those serving abroad. Although a specific number is hard to pin down, the State Department receives roughly $15 million a year,

including $10 million to increase security at American and international schools abroad. All State Department employees now receive basic security training, including crisis response and self-aid and "buddy care" through programs like Simple Triage and Rapid Treatment. Those stationed overseas are given enhanced training on the local threat through the Security Overseas Seminar (SOS) Program. The Security Overseas Seminar, which concentrates on life in overseas environments, is mandatory for all federal employees and recommended for eligible family members. A similar, age-appropriate program, Young SOS, is offered to young family members in grades 2–12.

Under the Soft Targets Program, the State Department is spending $27 million to improve the protection of US officials and their families at Department-assisted schools from terrorist threats. This multiphase program provides basic security hardware such as shatter-resistant window film, alarms, and radios, and additional protective measures designed based on the threat levels in the country. Also, security walls, bollards, and gate systems were funded for the schools. As a parent of a high school student attending one such institution in the Middle East, I am eternally gratefully for the funding my government has expended to keep her safe while we serve in our military assignment.

Ambassador Bushnell also recognized the culture must change along with the shift to protect the State Department's soft targets. She made three prescient recommendations that are applicable to all sectors:

1. Finding the right balance between living vigilantly and normally. People do not stay on high alert for long periods of time. Scare tactics are ultimately self-defeating, and administrative mandates such as checklists risk becoming rote exercises. To use a metaphor, our challenge is to ensure people are looking both ways before they cross the street, becoming neither paralyzed nor indifferent to the oncoming traffic.
2. Maintaining a consistency of funding and attention to security issues.
3. Changing the ethos, perception and the image of the job. Employees can count on experiencing evacuation, civil unrest, kidnapping, natural disasters, assassination, terrorist attacks, biochemical attacks, and other crises.

Certainly the State Department's mission overseas is far more vulnerable to terrorist attack than a school in the US heartland. However, the Ambassador's insight as someone who lived through an unexpected and unanticipated terrorist event against a hard target is thought provoking and a departure for further discussion. She ended her testimony with this statement: "My colleagues are fiercely patriotic, willing to put themselves and their families at risk in order to make a difference on

behalf of the American people. At the very least, they deserve our best efforts to keep them safe."

UNITED NATIONS AND SOFT TARGETS

The United Nations has also entered the soft target hardening realm around the world. The organization's preferred manner of engagement is through a program called Public–Private Partnerships (PPPs), for the protection of vulnerable targets against terrorist attacks (UN 2009). Through its Counterterrorism Implementation Task Force (CTITF; http://www.un.org/en/terrorism/ctitf/wg_vulnerabletargets.shtml), the UN's PPP task force harvests best practices, leveraging the connections and insights of INTERPOL about threat and response. INTERPOL also ensures timely dissemination of threat and attack information through the PPP construct. The UN also runs a Major Events International Academy aimed at those responsible for managing and securing high-attendance events such as the FIFA World Cup, Wimbledon, and multiday stadium concert events which are popular in Europe. Recognizing that event owners must ultimately decide how to secure their venues, the academy provides a good model for staying engaged and being a conduit for information and training, without imposing its will. Because the United Nations must respond during attacks such as the Boko Haram kidnapping of female students in Nigeria and the Westgate Mall massacre, they are investing money and time up front to help prevent soft target attacks around the world.

The State Department's Overseas Security Advisory Council (OSAC) is a PPP to promote security concepts and enhance cooperation between the state and US organizations operating worldwide. OSAC focuses in particular on soft, vulnerable targets and provides a forum for the exchange of best practices and a platform for the regular and timely interchange of information between the private sector and the Department of State. At the city level, one very successful PPP is Project Griffin in London, a joint venture between the City of London and the London Metropolitan Police forces. Its charter is to advise and update the managers, security officers, and employees of large public- and private-sector organizations across the capital on security, counterterrorism, and crime prevention issues. The initiative focuses on protecting the city and the public from terrorist attacks. It brings together and coordinates the resources of the police, emergency services, local authorities, business, and the private-sector security industry, and helps with implementation of counterterrorism and crime prevention policies and procedures. Awareness and reporting of hostile reconnaissance and other suspicious activity have been dramatically increased across London since the implementation of Project Griffin, and this initiative could surely be replicated in our cities.

The Department of Justice (DOJ) has an Office of Community Oriented Policing Services that hosts PPP initiatives called "Building Private Security/Public Policing Partnerships to Prevent and Respond to Terrorism and Public Disorder." Community-oriented policing can help control crime. The private sector and community members are encouraged to participate actively in the development of prevention strategies including those designed to counter terrorism. The DOJ is helping with the development of knowledge resource products (CDs, guidance documents, and videos) as well as training individuals from the public and private sectors.

The UN's PPP initiative is powerful because it enforces a critical concept related to soft target protection: the role of the private sector should not be limited to involvement in crisis situations. A proactive approach to partner and develop measures to prevent terrorism and enhance overall security can prevent and/or deter attacks. Of course, the type of threat information the government can share with the private sector is an issue and the sector must understand the importance of safeguarding such information. Also, law enforcement should not merely share threat information, but also assist with identifying and mitigating vulnerability. A trusting relationship is the key to successful PPP partnering.

There is much to harvest from soft target hardening efforts around the world, especially through the sharing of best practices. Now, with knowledge of the threat, vulnerability, and worldwide response efforts, we can move forward to address hardening planning and tactics here at home.

REFERENCES

CNN. "Color-Coded Threat System to Be Replaced in April." (January 26, 2011).

Cobb, Sean E., Air Force Master Sgt. "Bronze Star Awarded to Airman for Combat Actions." (December 21, 2005).

Gichuhi, Francis. "Terrorism in Hotels and How to Prevent Attacks through Design." *A4architect,* May 14 2014.

Hesterman, Jennifer and Sarah Kinzer. "PG&E Sabotage." *The Counter Terrorist Magazine* (June 2014): 18–29.

UN (United Nations). "Counter-Terrorism Implementation Task Force." http://www.un.org/en/terrorism/ctitf/wg_vulnerabletargets.shtml (2009).

———. "Public–Private Partnerships (PPPs) for the Protection of Vulnerable Targets." Edited by Counterterrorism Implementation Task Force, 2009.

US House of Representatives. "Overseas Security: Hardening Soft Targets," May 10, 2005.

CHAPTER 8

Soft Target Hardening 101

Security is always seen as too much until the day it's not enough.

—William Webster, former FBI director (2002)

INTRODUCTION

Mr. Webster made the preceding statement during a debate entitled "National Security versus Personal Liberty" on March 3, 2002, at the UC Santa Barbara. The balance of security and human rights is important as we seek to secure our facilities and events. Terrorism, by its very nature, is a violation of human rights. However, when we become heavy handed in the face of a terrorist threat and overreact, stripping away elements of the very democracy our enemies seek to destroy, we have played into their hands.

Physical profiling is a counterproductive tool in postmodern terrorism and we must dismiss the notion a terrorist "looks" a certain way. After 9/11, the law enforcement community focused on foreign-born male Arabs; yet we soon learned radical jihadists can be American non-Arabs and, in some cases like Jihad Jane, a woman. Although hard for us to conceive, the use of women, children, and the disabled is another proven asymmetric tactic shared among terrorist groups worldwide. In 2008, two disabled women were unwillingly used by al-Qaeda in Iraq to attack an open market in Baghdad; the devices were strapped to their wheelchairs and remotely detonated. Also in Iraq, a female suicide bomber attacked a group of women and children at a playgroup gathering, killing fifty-four people. In 2011, a man dressed as a cleric and a small boy were walking toward a government building in Karachi; alert police approached the pair and found they were both wearing bomb vests. In 2012, a fourteen-year-old suicide bomber walked into a group of his friends playing outside the NATO building in Kabul, Afghanistan, killing six.

Profiling by age also does not work in the United States, as the al-Qaeda in America study covered in Chapter 4 illustrated—radical Islamist terrorists in our country have ranged from nineteen to sixty-three years old. Profiling can also lead to tunnel vision: while we are focused on one group or demographic, the real threat is on the periphery, taking advantage of our myopia. We also must take care when profiling based on a person's activities, which may be quite harmless, such as taking photographs or sketching locations. Our efforts can lead us down a wrong path, distracting and expending resources while infringing on a person's rights in the name of security. Certainly, calling law enforcement is prudent if the situation exceeds what you can handle; however, be aware that if the Joint Terrorism Task Force becomes involved, suspicious activity reports (SARs) filed with the FBI on an individual may be held for up to twenty years. Perhaps a popular saying in the security realm applies: If everyone is a terrorist, no one is a terrorist.

Furthermore, our hardening activities may unconsciously legitimize the terrorists or aggrandize them in a way where their power grows. For example, thanks to Richard Reid, the "shoe bomber," we all now have to take off our shoes at airport security. After Umar Farouk Abdulmutallab, the "underwear bomber," tried to detonate a device in his pants, the restriction on carry-on liquids was put into effect. The backscatter machines may deter the one bad actor who is thinking about an airliner attack, yet inconvenience and intrude on the privacy of millions daily. Certainly these knee-jerk overreactions and the understandable outrage by the flying public must delight the terrorists: our way of life changed = they won.

Finally, our asymmetric enemies keep reinventing tactics and improving, so we must not only tighten security based on past events, but also be aware of what is happening worldwide and prepare for copycats here in the United States.

STEADY-STATE AND CRISIS LEADERSHIP

So now you may be thinking:

> Profiling will not work. I do not want to make my facility into a fortress. The security environment is dynamic and unlike a government building, I cannot merely barricade my buildings and occupants into a cocoon of safety. The threat keeps changing as groups shift tactics and learn based on past successes and mistakes and I do not have the resources for high-end equipment and a legion of guards. How should I proceed?

Security begins and ends with the decisions and actions of the organization's leadership—not just the front office but also everyone who has a key role on the leadership team. "Steady-state operations" is

military vernacular describing periods of predictable activity, the day-in and day-out rhythm of an organization. During steady state, the leader ensures the organization trains, equips, plans, and practices. In terms of training, there are outstanding resources regarding threat, vulnerability, risk management, emergency response, and hardening for owners, operators, leaders, staff, and building users. For example, Appendix B contains a list of free FEMA certificates and courses open to everyone, many of which also give credit hours for security certifications and college degree programs. Also, the Red Cross can always come to the facility and give first aid, CPR, and emergency medical care training. The fire department would be happy to inspect your facility for hazards and law enforcement can assess the security of your property and building. During quiet periods, you may want to upgrade your security system, add a few cameras, and implement other suggestions you may find in the next chapter. Dust off your emergency plans and checklists and gather your key people to "what if" scenarios and talk through response. The point is that during steady state, you build and tend to the foundation which will hold you, your team, and the organization afloat during a crisis.

Crisis leadership is when you will rise to the occasion or fail; there truly is no in-between state. If danger crosses your doorstep, there will be a full investigation and history will judge your actions and inactions. As leaders, we may get the glory for the wonderful things that happen in the organization, but we are also held accountable for its failures, especially if they involve loss of life. Often, leaders fail during crises because they were not mentally or physically prepared for the acute stress of the situation, mainly because they chose the easier path of invulnerability: "It will never happen to me," and "It will never happen here." We all have our stories about the fateful day of the 9/11 attacks, but perhaps mine will help provide perspective in terms of fifteen years of steady-state training, planning, equipping, and practicing and how it paid off.

September 11, 2001, began as all other days, with a morning office meeting to discuss the daily schedule and downing a few cups of coffee to fuel the way ahead. I was an Air Force lieutenant colonel, stationed at Seymour-Johnson Air Force Base, North Carolina, an Air Combat Command base with several squadrons of F-15E fighter aircraft and thousands of military personnel and their families. We were gathered around the office television to watch live video of the "aircraft accident" in New York City and the increasingly thick smoke pouring out of the north tower of the World Trade Center. At 9:03 a.m., a collective gasp filled the room as we witnessed the second aircraft impacting the south tower. The mood immediately shifted from concern to horror with the realization that our country was under attack. And I instantly knew, from years of research and study, the attacker was unmistakably al-Qaeda.

Suddenly, I was in the unexpected position of trying to secure a major military installation and its panicked residents from an enemy with unknown intentions and capabilities. In the command center, my stunned colleagues and I watched the defense readiness condition change to DEFCON 3, the highest level since the Cuban Missile Crisis. The Pentagon, which I had just left three months earlier, was attacked and burning. I had to suppress thoughts about my E-ring office and many colleagues in danger or possibly dying. With more hijacked aircraft airborne, our fighter jets were immediately loaded with weapons and crews put on alert. My husband, then a colonel, commanded the fleet of fighter aircraft and crew members; before allowing them to take off, he had to make sure his pilots were prepared to shoot down a civilian airliner on command: something they had never trained for or considered a remote possibility prior to this fateful morning. We soon received the order to launch, and I could hear the aircraft thundering into the skies to fly Combat Air Patrol sorties over major East Coast cities to guard from further attacks.

My job at the helm of the Emergency Operations Center was chaotic for the next thirty-six hours. As the installation gates were locked down, we had children (including our young daughter) outside the fence in community schools and worried parents who were trying to get to them. We had scared citizens from the local community asking for refuge on the secured base. Landlines and cellular phone networks crashed, and our most reliable way to communicate was through handheld radios, known as "bricks" for their cumbersome bulk. I ordered the communications squadron to break into deployment kits and access every other storage area on base to harvest "bricks," batteries, and charging stations for commanders and first responders. Upon wise counsel from a staff member, I immediately executed a long-standing contingency contract to withdraw bottled water from the base commissary for safekeeping in case the installation became a self-sustaining island. Sure enough, within hours, the grocery store was inundated with base employees and family members who understandingly stripped the shelves of basic essentials. My security forces defenders established force protection delta posture, the highest possible, emptying the base armory of battle gear, M-16s, and service revolvers. Snipers and countersnipers took position around the base to protect us from attack. As I watched the surreal situation unfold, I remember thinking the hundreds of mundane exercises endured during our careers had paid off. We were a calm, precise, well-oiled machine during the most intense stress of our young lives.

As I executed seven binders of emergency checklists, my team was faced with several unanticipated threats, starting with the escape of an inmate from a minimum security federal prison on base. A convict with an "interesting" background had taken advantage of the 9/11 morning confusion to jump the base fence; a quick check of records revealed that

he routinely participated in work details all over the base, in unclassified facilities and along the flight line, mowing grass, picking up trash, and likely interacting with base personnel. The standard operating procedure was to put up search helicopters; however, the state police were denied flight clearance due to the national emergency. Instead, we implemented a coordinated ground search with local sheriffs, but without further intelligence about the 9/11 attackers, we were flying blind. The prisoner's intimate knowledge of our base and possible intentions were of extreme concern.

A few hours later, an FBI agent from a local office requested a secure phone call with our military federal agents, residing in the base Air Force Office of Special Investigations (AFOSI). We listened with surprise as his staff described ongoing surveillance operations and suspicious activities within the state and at nearby facilities, some frequented by military personnel. The base was suddenly not the secure "island" it had always seemed. I also quickly learned to operate within a new realm, that of ambiguity and the "inescapable unknowables." Thankfully, no threats to the installation materialized in the coming days, and eventually our attention shifted from protecting the homeland to taking the fight 7,000 miles away to the enemy.

Some of the security measures we put in place were painful and inconveniencing. Naturally, on the day of the attacks and for a few weeks afterward, people did not complain about the long lines at the base gate or having to wear extra body armor and carry gas masks. However, as time went by and there were no additional attacks, security fatigue set in. Even military members and their families became irritated and less cooperative. The problem from a threat standpoint is that with asymmetric attacks—when terrorist groups act at will on the day and time and at the place of their choosing—we do not know if the threat has subsided. Are they regrouping and planning? Will the next attack be a weapon of mass destruction (WMD)? Or was this their one big operation and the culmination of a decade of planning and fund-raising? No one knows the answers to these questions, not even our nation's director of national intelligence. So we lowered the security posture, taking baby steps back toward where we were on 9/10, trying to re-establish the balance of security and normalcy.

As previously discussed, the leader must identify vulnerabilities in the face of the threat and acknowledge and accept risk as needed. Chapter 9 gives some ideas for how to work through these issues, but perhaps think about the one "Achilles heel" in your organization that, if leveraged by the adversary, will have the greatest impact on the safety and security of your facility and its occupants. In an organization that cannot control access, such as a college campus, perhaps it is an active shooter on foot or in a vehicle; research examples such as the sniper

at Penn State in 1996 and the UC Santa Barbara campus shooting in 2014. In situations with tight access, such as sporting events and concerts, open-air venues are vulnerable from the skies, and closed venues through their ventilation systems. Food operations are always a risk. A megachurch with a few entrances may identify its weak spot as the central air conditioning ventilation system or an arson event. The hospital emergency room may be the most vulnerable place in the building; however, the main entrance must also be protected by an alert front desk staff looking for the first sign of a problem.

A resource-constrained operation should try to identify security tactics and equipment that will have the greatest impact in terms of saving lives. A "cafeteria" option—choosing from a wide slate of ideas and best practices—is also a possibility. Chapter 9 provides a slate of hardening tactics and checklists as a point of departure for your organization. The ambiguity of modern terror dictates, however, that soft targeting can be random and unpredictable—an attack conducted by an opportunist who is enraged and pushed to act on his or her impulses at your facility. The attack in the parking lot of the Jewish Center in Kansas City, Kansas, by an enraged white supremacist provides the best recent example of little to no planning and acting out of rage. Also, remember history may not be the best predictor of soft target strikes; for example, prior to the shooting at Virginia Tech, there was no other event like it in our country. Prior to the Beslan school massacre or the Moscow theater siege, there were no similar prior events. This is why soft targeting is a true black swan: nothing in the past could predict the situation we may find ourselves in today.

INTUITION

One of our most underappreciated natural gifts is our intuition or the ability to know something from instinctive rather than conscious reasoning or proof of evidence. Almost every case study in the book contains statements from either the families of the perpetrators, their friends, colleagues or people at the scene saying "Something just didn't feel right," or, worse, "I knew something like this could happen" or "When I heard about the shooting, I knew it was him." Trust your gut feeling, honed by years of experience and wisdom. If something looks or feels wrong, it likely is. The US military has done a great deal of work on intuition, especially the Marine Corps, which includes honing and trusting the sixth sense as the "art" in the art and science of war discussed in their doctrine. Based on stories from combat veterans returning from Afghanistan and Iraq about situations where intuition saved countless numbers of lives on the battlefield, the Office of Naval Research is launching a study in late 2014 on how military members can hone their

intuition: "Research in human pattern recognition and decision-making suggest[s] that there is a 'sixth sense' through which humans can detect and act on unique patterns without consciously and intentionally analyzing them" (Office of Naval Research 2014).

As discussed in the previous chapter, terrorists and criminals will often accomplish surveillance at the target prior to acting, sometimes returning to the scene more than once. It is within your right as the facility operator or manager to ask a stranger if you can help him or her, and this gives you a chance to assess verbal and nonverbal behavior. Also, the entire staff can be force multipliers in this regard. Naturally, if the individual looks threatening, it is best to call security or the local police department instead of confronting the stranger. After any suspicious event, take notes on the person's physical appearance and what he or she was wearing and carrying. If the person drives away, note the make and model of the car, and even the license plate number. You will probably never need the information, but it will be of great help to investigators if your gut feeling was correct. Also, if the individual was an opportunist, the mere fact you engaged and saw him or her may deter further actions. Again, as with all hardening activities, you may never know the impact of your actions.

INSIDER THREAT: A FIFTH COLUMN

As if the soft target hardening situation was not already complex enough with myriad actors and tactics, we need to factor in the growing insider threat to organizations. When you ask a security professional the question, "What keeps you up at night," the insider threat is likely the answer. In military terminology, the insider threat is a "fifth column"—a group of insiders who secretly sympathize with or support an enemy and engage in acts of espionage or data gathering for the larger group's planning efforts, or subversion, thus destabilizing the organization from within and further "softening" the soft target. Consider the sabotage perpetrated by insiders Edward Snowden and Bradley Manning; they never pulled a trigger, but certainly put many others in the crosshairs with their sharing of extremely classified government information with the world, which includes state enemies and terrorist groups. The insider could also be a "lone wolf"—perhaps the most dangerous situation of all as planning activity will often go undetected. Know that the insider is a force multiplier to an attack, with intimate knowledge of your facilities, operations, and vulnerabilities. This individual can also pre-position supplies for himself or herself or others, as well as assess the perfect time to strike and obtain the maximum results, whether casualty counts or damage to the physical plant or the organization's reputation.

There is a persistent lack of research and data analysis regarding the insider threat, making it the least understood and least appreciated danger to an organization or venue. Compounding the problem, there are organizational and cognitive biases that lead managers to downplay the insider threat. Indicators we use to detect threats with outsiders fall short and our countermeasures fall short; we inherently trust the insider and he or she has a legitimate job and role in the workplace. There is a myth these employees are disgruntled or have outward signs of hostility at work; although some workplace attacks occur by recently fired employees, many others come as a complete surprise. Risk assessments usually do not include insider threat, but they must to protect the organization or venue and its occupants fully. Add it to the top of your list of risks.

Good Hiring Practices—First Line of Defense

Countering the insider threat takes a multifaceted approach. The body of academic work regarding the insider threat is fairly small, but I strongly recommend the book, *Managing the Insider Threat: No Dark Corners,* by Nick Catrantzos (2012). He applies the Delphi methodology to this security challenge and arrives at the conclusion that infiltrators are more likely to be a threat than disgruntled insiders. In other words, the terrorist or group is more likely to try to plant one of his, her, or its own than to leverage a disgruntled insider (although the threat of the latter must not be overlooked). First, the infiltrator needs to get through your screening process and then on the payroll and into your facility. Certainly, a thorough employee background check is necessary, and I recommend using an approach similar to that used in the government's security clearance process. In terms of past employment, absolutely call past employers, but do not ask only about the former employee's work ethic, etc. Take the opportunity to probe a little. Perhaps, in the name of security and the workplace violence issues in our society, ask about the emotional state of the employee and whether there were any signs of anger or disloyalty. At the end of the discussion, ask an open-ended question: "Is there anything else you think I should know about this person?" When interviewing the potential employee, stay within the law but ask everything you can about background, family, and even financial status.

You should strive to apply psychometrics to your hiring process; there is plenty of information on the Internet about these practices, and you can hire an external company to do all of your pre-employment screening. But know that the screening process itself has many flaws; deception experts believe 40 to 50 percent of applicants lie on their resumes and job applications and 80 percent lie during the full screening interviews (Whetstone

2014). The potential employee is likely trying to impress the hiring official by inflating past work experience or abilities or, possibly, he or she does have something to hide that might preclude hiring. For those who try to read body language during an interview, untrained screeners are usually about 50 percent accurate, but body language deception experts are 80 to 90 percent accurate. Therefore, a pre-employment screening by experts is a good frontline of defense for your operation.

Background Checks

The National Employment Law Project (NELP 2014) estimates 65 million US adults, or one in four, has an arrest or conviction record, though not all of these are felonies. The federal government has passed laws to allow businesses and organizations to conduct the background checks on potential employees who will come in contact with children in schools, churches, and hospitals. These checks are often performed by both state and federal law enforcement, often through simple fingerprinting and processing at the local police station, which will determine whether the person was ever convicted of a crime. Be advised that this system does not indicate other previous arrests or instances where the charges were dropped. As for other businesses, you may or may not be able to run background checks. However, the employment application (private and confidential) should include a questionnaire regarding the applicant's criminal history. If your state or church only requires a state-level check, then keep in mind that you will not receive any information from a crime committed outside that state. Also, a new movement is not in your favor: ten states have passed "ban the box" laws barring employers from asking potential employees about past convictions, believing the information creates an unfair barrier to employment. Also, more than sixty city and county governments, including Atlanta, Indianapolis, and Kansas City, Missouri, do not allow the practice. Therefore, you may need to complement your screening process with professional help and through Internet searches and other legal avenues. The time and money involved with verifying the background of an employee are worth it.

After gaining employment, the mole, as we refer to the nefarious insider here, must gather information and determine how best to exploit your vulnerabilities. Detecting a radical jihadist or other religious or political ideology is more difficult than detecting outright anger. Mole hunters are used by the government to find spies in an organization; perhaps one of the best books I have ever read on this topic is *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy*. The author, Scott Carpenter (2007), was a mole hunter at the Defense Intelligence Agency; his sole job was to identify insiders

who were colluding with or spying for other governments (the "fifth column"). In the book, he is honest about how he failed to act upon his early gut feelings regarding Montes, who, interestingly, was recruited while a night school student in a master's degree program at Johns Hopkins. By Carpenter's not acting on his instincts, Montes was able to spy for Cuba several more years, and the intelligence she gave them resulted in the deaths of several Americans at a classified outpost. Carpenter retrospectively looks at the case and the indicators that Montes was not a "friendly," despite her ability to pass two polygraph tests.

The "no dark corners" approach offered by Catrantzos (2010) in his work illuminates the work space. First of all, a cultural shift is needed: all of your employees should be seen as force multipliers in terms of security. One person in an organization does not "do" security; rather, everyone is responsible for securing the workplace. Therefore, hire your employees on a probationary basis and treat the situation like a pilot/copilot scenario; stay close or have one of your long-term, trusted employees act in the mentoring role. The "no dark corners" concept means new employees are never left alone during this "on-boarding" period, thus communicating to the insider that "someone" is watching at all times. The workplace should be very transparent in terms of physical work spaces and redundancy and accessibility. Other than the manager, employees should not be the sole source of information or access; for instance, one person has a combination to a safe or a person has an e-mail account or files to which only he or she has the password. In the spirit of transparency, have regular audits in the workplace, that way if you suspect an employee is an insider threat, it is easier to approach and gather evidence prior to calling for outside help. The chart in Figure 8.1 shows the innovation of the "no dark corners" theory for securing against the insider threat.

The "no dark corners" approach might also be taken from a facility standpoint, with manager and security personnel regularly walking the perimeter looking for cut fences or other indications of stockpiling or operational planning. Every storage area and compartment should be routinely inspected—again, to look for stockpiling. Look up at ceiling tiles and down at floorboards, and at everything in between. Employees have the right to privacy, but construct an open area where the work space is visible, including the computer screens. Several cases already discussed in this book involved insiders pre-positioning explosives and weapons in the workplace, sometimes over the course of months. Staying vigilant will not only deter the insider but also, it is hoped, detect their activity early in the planning cycle.

Much work has been done to mitigate the insider threat from a critical, secretive, isolated workplace: nuclear power plants. Insider threats are the most serious challenge confronting nuclear facilities, and in every

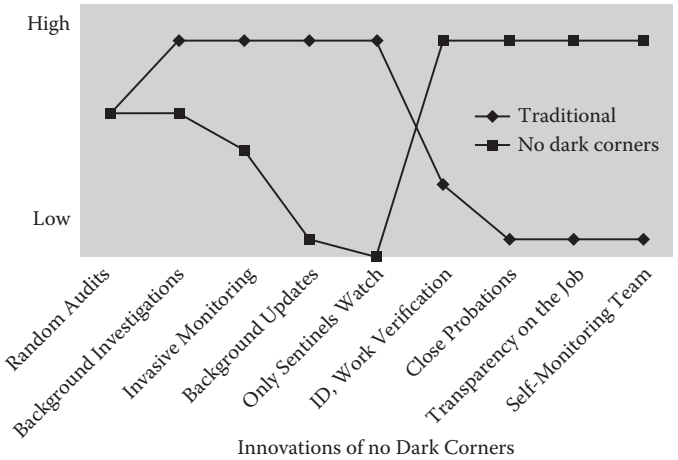


FIGURE 8.1 The "no dark corners" approach. (Catrantzos, Nick. "No Dark Corners: A Different Answer to Insider Threats." *Homeland Security Affairs Journal* VI (2). May, 2010. With permission.)

case of theft of nuclear materials the perpetrators were either insiders or had help from insiders. Sabotage is also a threat; in 1982, an employee detonated explosives directly on a nuclear reactor at South Africa's Koeberg nuclear power plant and in 2012 an insider sabotaged a diesel generator at the San Onofre nuclear facility in California. Matthew Bunn and Scott Sagan (2014) authored a very informative piece about worst practices and failures in the industry regarding the insider threat, with takeaways that may be cross-applied to soft targets. The authors encourage facility owners and security managers to fight their assumptions, stating:

- Don't assume that serious insider threats are NIMO (not in my organization).
- Don't assume that background checks will solve the insider problem.
- Don't assume that red flags will be read properly.
- Don't assume that insider conspiracies are impossible.
- Don't assume that organizational culture and employee disgruntlement don't matter.
- Don't forget that insiders may know about security measures and how to work around them.
- Don't assume that security rules are followed.
- Don't assume that only consciously malicious insider actions matter.
- Don't focus only on prevention and miss opportunities for mitigation.

Fighting these assumptions, use of psychometrics in the screening process, and the "no dark corners" approach will go a long way toward thwarting the insider threat.

Many soft target venues use volunteers, whether in school libraries, running church groups, staffing the reception desk at a hospital, or during sporting and recreational events. Due to budgetary woes, organizations may even replace paid staff and use volunteers in key front office positions. Someone with nefarious plans may think volunteering is one way to get inside an organization and its facilities by skipping the employment background checks. Apply the same rigor to checking the background of your volunteers and always have your staff do a face-to-face interview to pick up on any deception or gut feelings.

KIDNAPPING AND THE USE OF HUMAN SHIELDS IN TERRORIST OPERATIONS

The cases of Beslan and the Moscow theater siege have been the largest terrorist kidnapping and hostage-taking crises at soft target venues; however, there have been dozens of others and the tactic is escalating among terrorist groups. Not only al-Qaeda, but all of the international terrorist groups, as well as Mexican cartels, routinely kidnap tourists as a way either to raise ransom or to secure the release of imprisoned colleagues. The recent trend is that even if the ransom is paid, hostages are not released per the agreement or are killed anyway. Also on the rise are parental kidnappings during custody battles, a crime that schools and daycare providers must secure against.

Managers and security personnel at soft target facilities and venues should also prepare for the possible use of children, women, and the elderly as human shields by terrorists (international or domestic) on our soil. Human shields tactics are the deliberate placement of civilians around targets or combatants to prevent the enemy from firing. The use of human shields is prohibited by the Fourth Geneva Convention, Protection of Civilian Persons in Time of War, which was passed in 1949 as a result of atrocities perpetrated by the Nazis during World War II. Specifically, the article states (http://www.icrc.org/ihl.nsf/WebART/470-750065?OpenDocument):

> The presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favour or impede military operations.

However, as discussed in Chapter 2, terrorists do not adhere to Geneva conventions or worry about worldwide condemnation of their

activities and therefore routinely use this tactic when facing law enforcement or military response at the scene of their attack.

Several terrorist groups that have previously attacked Americans and have operatives in the United States and/or Canada use human shields. Independent reports give detailed evidence Hamas used hospitals, schools, homes, and mosques to hide weapons and soldiers during the Gaza War, an Israeli military initiative from December 2008 through January 2009. At twenty-five miles long and six miles wide, with a population of 1.5 million, Gaza is the sixth most densely populated place on earth, providing a very complex battleground situation. The UN report on the war mentions the possible use of children, women, and the elderly as human shields by Hamas; however, Malam, an Israeli intelligence think tank, produced a report using declassified material such as videotapes, maps, and operational plans recovered on the ground by Israel Defense Forces troops. The information indicates Hamas hid improvised explosive devices in and around civilian homes and hospitals, and video taken from a helicopter appears to show the use of children and the elderly as human shields for soldiers engaged in operations.

The Liberation Tigers of Tamil Eelam (LTTE) were defeated by the Sri Lankan government in May 2009 in a final, violent offensive on a northern beach in the Vanni region. During the months leading up to the conflict, the United States used satellites to monitor the situation, releasing photos to the public to show how LTTE herded hundreds of thousands of citizens on the beach for use as human shields in their final standoff with government forces. Many died from starvation, execution, or government shelling, and some escaped only to be captured and put into government internment camps. The remaining civilians, approximately 130,000, were forced to stay in a one-square-mile area of beach and be part of the final battle. There has been no final accounting of civilians killed in the final offensive; the United Nations (2011) estimated at least 40,000. A BBC documentary entitled *Sri Lanka's Killing Fields* documents the atrocities performed by the government and the rebels in "no fire" and "safety" zones, as well as hospitals, schools, villages, and convoys of refugees deliberately pulled into the conflict (Snow 2011). In 2012, a Sri Lankan general admitted to war crimes, including the extrajudicial killing of civilians. According to intelligence agencies, LTTE members who fled the country are regrouping in Canada.

Although it seems inconceivable to us that a terrorist group, cartel, or lone wolf would use human shields, we must remember the power of ideology, especially radical religious dogma, which empowers believers with a sense of justification for their illegal and immoral activities. The Beslan example reminds us the terrorists will use civilians to absorb the line of fire. Naturally, it is difficult to "go there" mentally, but we should

prepare for even the most horrific of scenarios, including the terrorist exploitation of innocent civilians to further goals.

SURROUNDED BY CRISES

Often, soft targets are in the area or even on the grounds of a hard target; they may not be part of the scenario, but get pulled into the disaster by virtue of location or services provided such as shelter, religious comfort, or medical care. In October 1997, LTTE terrorists arrived on the scene at the newly inaugurated World Trade Center in Colombo, Sri Lanka, with its twin thirty-nine story towers as the target. However, the attackers could not get their truck bomb into the building's parking lot as planned. Instead, they parked next door, at the Galadari Hotel, and detonated the device by firing rocket-propelled grenades into the vehicle. The Murrah Federal Building in Oklahoma City had child daycare onsite, which unfortunately was on the bottom floor of the building and took the brunt of the blast from the 1995 domestic terrorist attack. On 9/11 there was a large daycare center located just a few hundred yards from the Pentagon. As previously discussed, there were a number of schools located near the Twin Towers, and nearby churches were pulled into the attack by being blanketed by toxic dust and used as mortuaries and sanctuaries for weary and devastated citizens and first responders. During the 2012 unrest in Libya, US government officials identified a hotel and ordered all Americans to use it as an evacuation rally point even though the hotel was not consulted, putting its employees and guests directly in the line of fire. Even natural disasters can quickly turn into a period of unrest and violent crime that impact our facilities. For example, during Hurricane Katrina in August 2005, the Louisiana Superdome was used as a mass shelter of "last resort," becoming a cesspool of sewage, vandalism, a suicide, possible murders, and reported rapes and gang activity.

Several scenarios are ripe for discussion: What if there is a terrorist attack unfolding in your town or city during the school day or a church service? How do you shelter in place and protect your building occupants? Do you open your doors to those fleeing the event, possibly bringing the attacks to your property? Do you share your supplies? What if the event lasts three days? During Hurricane Katrina, Keesler Air Force Base, Biloxi, Mississippi, was the only location in the area that had some electricity (thanks to emergency generators and fuel) as well as water and food. After the crisis, people in the devastated town wandered to the base gates to see if they could get help. On 9/11, confused and upset people were congregating at churches and schools, which naturally opened their doors. These are difficult scenarios, but thinking through

them is critical to response during crises. In the event of a criminal- or terrorist-related emergency in the community, you may want to turn off lit signage, decrease interior lighting, and lower profile. Also, investigate "contingency contracts" with local water and food delivery companies in case you are sheltering a group of people and the crisis goes on for an extended period of time. Similar to preparations for natural disasters, your organization may want to have a significant amount of cash on hand to purchase water, ice, and other necessities from stores if the electricity and ATMs are out.

FIRST RESPONSE AND THE THREAT OF SECONDARY ATTACKS

It is what people like us do: Without concern for our personal safety, we race to the scene of an attack to assist survivors, or we allow them entry into our secure sanctuary, be it our place of work or home. Law enforcement, chaplains, medical professionals, those with a military background—we are hard wired to respond this way, and our response is instinctive. Unfortunately, the instinct to run toward the fight, not away from it, could be deadly. My military colleagues often tell stories about the use of secondary and tertiary devices in Iraq and Afghanistan. The insurgents set off the first IED and wait until other soldiers rush in; then they set off a second device, sometimes a third. But this is not a new tactic; both international and domestic terrorists have employed it successfully for years. Facilities that often serve as shelters, such as schools, churches, malls, and sporting and recreation venues, can make themselves a target by assisting those fleeing a scene. As covered in Chapter 5, terrorists will even strike a hospital that is providing care to victims of the first attack.

International terrorist and criminal groups have successfully employed this "double-bomb" tactic to target first responders, and evacuating civilians are often caught in the fray. For instance, secondaries targeting responders in other notable attacks include the Jemmah Islamiyah hotel bombing in Bali in 2002, an anti-American attack by Hezbollah at the McDonald's in Lebanon in 2003, and the 2004 police station bombing in Athens by the Revolutionary Struggle group. In March 2010 in Dagestan, a Chechen suicide bomber dressed in a police uniform approached investigators and residents who had gathered at the scene of a car bomb explosion near a school and detonated his explosive vest. In April 2010, the primary al-Qaeda-related bombing in Algeria was followed by a secondary, detonated one hour later and killing a soldier. The same month, Chechen rebels bombed a train in Dagestan and remotely detonated a secondary device to target first responders.

Domestic terrorists also use this technique. Almost every attack perpetrated by Eric Rudolph included a secondary device specifically targeted toward emergency personnel. For example, prior to the Atlanta abortion clinic bombing in 1997, Rudolph called in a bomb threat and watched as office members evacuated and gathered in certain areas of the parking lot. He planned this into his operation months later; after he bombed the clinic, a second device went off an hour and a half after the first, injuring seven first responders. The Mexican cartels use secondary device tactics to ensnare and kill law enforcement. In fact, Louis R. Mizell, a terrorism expert and former US intelligence agent for the State Department, has compiled a database of three hundred double-bomb attacks by more than fifty terrorist groups in the world over the last ten years. His advice is "the reality of today's double-bomb tactic dictates that first responders have three primary jobs at a site: attending to the wounded, dispersing the crowd, and finding a second bomb" (Gips 2003).

The threat of secondary and tertiary bombing is real, and it must be factored into soft target hardening and emergency response procedures.

WEAPONS OF MASS DESTRUCTION

According to the FBI (2012), WMDs are defined in US law (18 USC §2332a) as

> (A) any destructive device as defined in section 921 of this title (i.e., explosive device); (B) any weapon designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; (C) any weapon involving a biological agent, toxin, or vector…and (D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. WMD is often referred to by the collection of modalities that make up the set of weapons: chemical, biological, radiological, nuclear, and explosive (CBRNE). These are weapons that have a relatively large-scale impact on people, property, and/or infrastructure.

Although we tend to worry about al-Qaeda groups using WMDs, chemical, biological, and radiological weapons are also on the table for use by domestic terror groups. A 2012 study conducted by Syracuse University's Maxwell School of Public Policy and the New America Foundation examined 114 cases of domestic terrorist acts and plots in the United States since 9/11, none involving al-Qaeda or groups/individuals motivated by Islamist radicalism. The ideologies studied span the spectrum from neo-Nazism and militant Christian fundamentalism to anarchism and violent environmentalism (New America Foundation

2012b). Among the vast number of weapons, destruction of property, and conspiracy charges, the research also found five plots of domestic terrorism involving chemical, biological, and radiological agents that could have killed thousands of Americans if executed (New America Foundation 2012a).

Naturally, al-Qaeda is at the very least interested in using WMDs against the United States. In the chemical and biological realm, a ten-volume *Encyclopedia of Afghanistan Resistance* found in Jalalabad contained formulas for manufacturing toxins, botulinum, and ricin and provided methods for dissemination. At Tarnak Farms, the former Afghan training camp near Kandahar, Afghanistan, al-Qaeda not only provided firearms training, but also experimented with biological warfare in a special laboratory. Ahmed Ressum, the Algerian al-Qaeda member who was caught at the Canadian border before he could execute the 2000 "millennium attack" of the Los Angeles airport, testified al-Qaeda taught him to poison people by putting toxins on doorknobs, and he engaged in experiments in which dogs were injected with a mixture containing cyanide and sulfuric acid. Also, al-Qaeda members were seeking to fly crop dusters that analysts believe might have been used to disseminate anthrax and chemical or biological agents (Boureston 2002). Regarding al-Qaeda and biological warfare, in 2009, Algerian newspaper *Anahar al-Jadeed* reported that forty AQIM (al-Qaeda in the Islamic Maghreb) terrorists died at a training camp in Algeria from their infection with bubonic plague (*Al Arabiya News* 2009). Speculation abounded: Was it a dead rat causing the deaths or an experiment gone bad? We will never know; however, al-Qaeda's *Inspire* magazine has encouraged its readers to manufacture ricin, botulinum, and sarin in their homes, even encouraging them to get a Muslim microbiologist to assist, if needed.

Finally, al-Qaeda splinter ISIS considered weaponizing Y pestis, or the bubonic plague in 2014, as indicated on a laptop seized from a militant/engineer in Syria. ISIS was keen to exchange American hostages for Pakistani neuroscientist Aafia Siddiqui, who is serving 86 years in US federal prison on terrorism charges. Also known as "lady al Qaeda," Siddiqui, who received her PhD in the United States, was captured in Afghanistan with detailed plans to construct a variety of WMDs and employ them against US targets. Therefore, it is very concerning that ISIS sought Siddiqui to become part of their campaign to expand their self labeled "caliphate."

Domestic terrorists may also use the al-Qaeda guides (widely available on the Internet) as a template for constructing their own weapons; in 2008, the FBI arrested Roger Bergendorff, who had ricin, a schematic for an injection pen, weapon silencers, and the jihadist *Anarchist Cookbook* in his Las Vegas hotel room. After recovering from ricin poisoning, he was sentenced to 3.5 years in prison. Bergendorff never gave

an exact motive behind his activities, but clearly it is dangerous to have private citizens tinkering with toxic biological and chemical compounds. We need to continue to work to get materials off the Internet and out of the hands of would-be attackers.

Perhaps the most accessible WMD is chlorine, an easily obtained chemical that could sicken or kill hundreds of people, under the right conditions. AQIM used chlorine in several vehicle-borne IED (VBIED) attacks against coalition forces in Iraq in 2006; although more casualties arose from the bomb blasts, the terrorists kept trying different methodologies to perfect their technique and used it thirteen more times in the war. Chlorine can be a silent killer; in 2005, two trains collided in Graniteville, South Carolina, in the middle of the night, releasing sixty tons of chlorine gas. Unsuspecting residents who heard the collision drove through the cloud, stayed in their homes, or kept working their outdoor night shift jobs. In all, nine people died and over two hundred fifty were sickened by the gas, which causes nausea, dizziness, and vomiting. Certainly chlorine is easily obtained; therefore, we have to educate suppliers on how and what to report in terms of suspicious buys or patterns. Facilities with pools should keep chlorine products stored in a locked facility.

Do al-Qaeda or other foreign and domestic terrorist groups have WMDs? Those of us who live in the "open source world" do not have the definitive answer to the question; however, we can turn to government reports and Congressional testimony to provide an accurate barometer. For instance, take the December 2008 report entitled "The World at Risk," issued by the Graham/Talent Commission, a bipartisan group that spent six months examining the WMD issue. When Senator Graham briefed Congress, he ominously stated, "Terrorists could mount nuclear or biological attack within five years." Statements from the report are also very telling:

> The commission believes that unless the world community acts decisively and with great urgency, it is more likely than not that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013. The Commission further believes that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon. (Commission on the Prevention of WMD Proliferation and Terrorism 2008)

Synthetic manufacturing is causing increased concerns, as chemically synthesized DNA can replicate DNA found in biological or chemical agents occurring in nature and, more worrisome, enhance the effects. According to Vahid Majidi, the assistant director of the FBI's Weapons of Mass Destruction Directorate, the agency is working to keep this

emergent technology from falling into the wrong hands (Committee on Homeland Security and Governmental Affairs 2011).

What does this mean for soft targets? WMDs have been used against civilians, notably the sarin gas attack by terrorist group Aum Shinryko (now known as Aleph) in 1995, which killed thirteen people, severely injured fifty, and causing temporary vision problems for nearly one thousand others, including first responders who rushed to the scene without the proper equipment. In the United States, Bhagwan Shree Rajneesh led a religious group in the Dalles, Oregon, area in the early 1980s. In an attempt to keep voters away from the polls and sway a 1984 local election toward a candidate friendly to the group, he and his followers deliberately contaminated salad bars at ten local restaurants with salmonella. The incident was the first and single largest bioterrorist attack in US history. Vulnerabilities of soft targets include contamination of the food supply in cafeterias and the use of central ventilation systems to release a chemical gas or biological toxins. Anthrax has been transported through the mail system to introduce it to the target area, so mail rooms should take extra precautions with suspicious letters or packages. A WMD agent might also be attached to a bomb, making it the dispersal method for radiation or chemical or biological agents. As illustrated throughout this book, WMD is in the playbook for a variety of bad actors wishing to do us harm; therefore, we must prepare.

IN THE SIRA METHOD

As previously stated, physical profiling efforts will likely come up short when identifying suspicious actors. However, behavioral profiling is a powerful tool as humans are unable to suppress certain physical changes that occur due to stress and adrenaline surges. Michael Rozin, the aforementioned Israeli security specialist who was also the security manager and captain of Special Operations at the Mall of America from 2005 to 2011, developed a methodology based on his experiences called the "Suspicion Indicators Recognition and Assessment" (SIRA)™. SIRA is an innovative behavior deterrence, detection, and security program, a proactive system to prevent acts of violence. Mr. Rozin believes (and I agree) there are some basic problems with the way organizations conduct their security program. The allocation of resources and effort is based on perceived threat level (e.g., "We've never had a shooting or a bombing here before, so the security posture is low"), there is a lack of comprehensive security assessment and design, and ineffective security objectives are in place. SIRA is based on human factors, in a complementary manner to physical security and security technology. Effective security objectives are to deter, detect, prevent, and respond; however,

tangible activities to deter, detect, and prevent are often given less weight than the response element. Mr. Rozin asserts the right approach is to believe the threat is constant; and an incident can happen at any time ("Today might be the day"). The relationship between suspicion and threat should be that suspicion is a threat until it is refuted. The approach should be, "If there is a doubt, there is no doubt." A doubt is a threshold for action and sometimes a doubt is reason for action. "Suspicious" does not mean "guilty"; the violent act is definitive evidence of guilt. There is a gray area involved with suspicions, but a preincident indicator is enough to take investigative action.

I strongly recommend the SIRA program for those responsible for securing soft targets as it provides tools for engaging when something does not seem right with an individual, whether a stranger or an insider. It draws on a leader's intuition, mentioned previously as an important security tool to hone and trust, and it gives permission and a methodology for engagement (Rozin 2014).

SUICIDE TERRORISM

Suicide bombings typically result in higher casualty counts because the actor can access areas packed with people or a critical place in the facility and detonate the weapon at the time of his or her choosing. Suicide bombings are a relatively new phenomenon; Islamic Jihad Organization's attacks in 1983 during the Lebanese civil war are the first examples of modern suicide terrorism. They have been used extensively as a war-fighting and propaganda tool by nearly every radical Islamist terrorist group in the last thirty years. Although suicide attacks amounted to just 3 percent of all terrorist incidents from 1980 through 2003, they were responsible for 48 percent of all fatalities, not counting deaths resulting from the suicide attacks via airliner on 9/11. In addition to strategically placed IEDs, suicide bombings are the primary tactic used in conflicts in Southwest Asia and are typically used against soft targets. In the ten years after September 11, 2001, there were 336 suicide attacks in Afghanistan and 303 in Pakistan, and there were a staggering 1,003 documented suicide attacks in Iraq between March 20, 2003, and December 31, 2010. Notable al-Qaeda suicide attacks since 9/11 include the July 7 attacks in London in 2005, which killed fifty-two people, and hotel bombings against US properties in Bali, Casablanca, Jakarta, Istanbul, Jordan, and Islamabad. Failed attempts at suicide bombing on airliners include the shoe bomber and the underwear bomber.

Suicide attacks can shift the center of gravity of a battle and break the will of fearful citizens. The effect is amplified when the suicide attack is against a soft target like an open market or a school. Rather than

focus on the psychology or motivation of a suicide terrorist, efforts are better placed on how to detect, prevent, and prepare for such an attack if it presents on your doorstep.

According to Dr. Daniel Kennedy (2006), a forensic criminologist, the following are seven signs of suicide terrorist activity (along with my elaboration); these steps can also be applied to detecting any type of terrorist or criminal preoperational planning activities:

1. Surveillance: The actor may observe the target area to determine security strengths and weaknesses, and the number of security personnel that might respond to an incident. Taking pictures, videotaping, drawing maps of the area, and stepping off distances are signs of terrorist surveillance activities. The 9/11 hijackers performed such surveillance on Disney properties and other soft targets. The Mumbai terrorists had a front man, American David Headley, who accomplished extensive surveillance on the targets. However, surveillance is not always necessary, as in the case of insiders or angry opportunists.
2. Elicitation: The actor attempts to gain information about certain operations: for example, asking questions about building infrastructure, class or worship schedules and attendance, and the posting of security personnel. The terrorists in the Nairobi mall shooting asked for and obtained blueprints of the building when securing shop space in the months prior to the attack.
3. Test of security: The individual may try to access unauthorized areas of your facility to test physical impediments or response time. Exit areas will be tested and possibly altered to prevent escape, such as in the Virginia Tech shooting when the shooter chained the classroom building escape doors closed; he was seen testing the chains the day before. David Headley walked the ground in Mumbai and knew every emergency exit at the hotels, later instructing the terrorists how to enter the building and block exits for high casualty numbers.
4. Acquiring supplies: The purchase or theft of explosives, weapons, ammunition, or security badges or uniforms in the local area is a red flag of possible impending attack. Insiders will also start stockpiling items in the facility such as in the case of the Westgate Mall attack.
5. Suspicious people: The actor may come to the future attack scene more than once. Looking out of place or wearing odd clothing, several of the perpetrators of mall shootings walked the same path they took the day of the shootings.
6. Trial run: Before the final attack, the terrorist may conduct a "dry run" to identify obstacles. A dry run might involve calling in a bomb threat to observe emergency response, evacuation plans, and rally points for those leaving the building, such as the tactic used by Eric Rudolph prior to the abortion

clinic bombing. Terrorists also may try to assemble weapons or bombs in the facility.

7. Deploying assets: In this last stage, the attacker and any operational supplies are moving or being moved into position. This is the last chance to prevent the attack.

When the planning begins, the suicide bomber has already decided to give up his or her life for the cause—whether revenge or a religious or political ideology. When backed into a corner, this type of attacker will jump straight to the execution stage of the operation, even if the timing is off, as has been witnessed in several suicide bombings where the individual was challenged before reaching the target and detonated the explosives. Therefore, never attempt to investigate, to engage, or to unravel any type of plot or attack on your own; call local law enforcement at the first sign of any of the preceding activity.

FACE OF RAGE

Your security personnel are your first line of defense, and they should be taught by experts to visually scan crowds or individuals for the following (Whetstone 2014):

- "Faces of threat" such as rage, anger, or guilt of a premeditated criminal act
- Threatening mannerisms
- Unusual nervousness
- Body language that could indicate having a concealed weapon

If your facility has a main reception area or front office, you may consider tailored training for those staff members. Anger is the most dangerous emotion; in this stage, a human is most likely to hurt another. Extreme anger, or unbridled rage, is extremely dangerous, as the capacity for rational thought and reasoning is lessened and the person will likely act out in a violent manner against the source of the rage until it is destroyed or the person is restrained.

Recognizing the "face of rage" is important in order to react properly to an imminent act of violence. Rage is an extraordinarily strong emotion, a feeling of intense, violent, or growing anger. There is a high adrenaline rush associated with a "fight or flight" response that can give extra strength and endurance; senses are sharpened and physical pain sensations are dulled. The enraged person may experience tunnel vision as he or she approaches the object of the anger. Due to elevated blood pressure, the person's sense of hearing will be diminished and he or she may actually "see red" due to bursting blood vessels in the eyes. Time may seem to slow, as the temporal perspective is also affected.

Rage is distinguished from other emotions by certain distorted facial expressions that cannot be reproduced and are the same regardless of race, ethnicity, or gender. The skin above the bridge of the nose folds in a certain way (think of the shape of the letter A), the lips become thin, and upper and lower teeth are visible. Also, the face remains fixed in a state of rage for approximately four hours before relaxing back to its normal state. Based on expression, which one of the people depicted in Figure 8.2 (interpreted from top to bottom and left to right) is the biggest threat to your organization?

- Picture 1: His face shows possible elements of rage, but because his hands are in the air, he better demonstrates "posturing," meaning he is mad and he wants you to know that he is mad.
- Picture 2: This is a good example of "stage 1 of rage," where anger is turning into rage. The man's eyebrows are scrunched together and he is showing the whites of his eyes, but the nose bridge of his face is not unnaturally wrinkled and his lips are pressed, indicating anger.
- Picture 3: This woman is showing "stage 2 of rage." The nose bridge is wrinkled, nostrils are flared, the white areas of the eyes are more profound, and the lips are beginning to separate.

FIGURE 8.2 Faces of rage. (Whetstone, Douglas. "'Catch the Lie': Importance of Body Language Deception Detection for Security Officials." Whetstone Security Group, Inc., 2014. With permission.)

- Picture 4: The woman is posturing, as evidenced by the display of her hand and arm. Her nose is crinkled and her upper lip is raised, which indicates disgust, not anger or rage.
- Picture 5: She is posturing and there is no scrunching of the nose bridge or the eyebrows being drawn together, which would indicate rage. The fact that her eyebrows are not lowered suggests she is not even truly angry.
- Picture 6: This face reflects anger, but not rage. Anger is best defined by lowered eyebrows and lips pressed together.
- Picture 7: His arm suggests posturing and there is no scrunching of the eyebrows or nose bridge, which would indicate rage. He is protesting and he wants you to know he is mad, but he is not in a state of rage and will probably not react violently.
- Picture 8: While this man is displaying a scrunched nose bridge, his raised upper lip is more indicative of disgust, not rage.
- Picture 9: The expression is not natural;, the picture is staged. The man is posturing, and the lowered eyebrows might suggest anger, except that the lips are not pressed together.
- Picture 10: This is a good example of "stage 4 of rage" due the scrunched nose bridge (with the letter A visible), showing the whites of the eyes, possible flared nostrils, and display of teeth with the lips forming a square. This is the look of animals (including humans) who are in unbridled rage and about to attack or are in the process of attacking.

For more information on reading facial expressions such as rage, I recommend *Unmasking the Face,* by Dr. Paul Eckman (2003), who is likely the best facial expression and lie detection expert in the world. Dr. Eckman consults to the popular television show *Lie to Me,* which uses his theories to explore criminal cases and deception.

As opposed to terrorist rage, which is aimed against those who represent an opposing political or religious system, criminal rage is more likely tied to low self-esteem where a person has been bullied or perceives ill treatment at the hands of others. A good example is twenty-two-year-old Elliott Rodger, who went on a shooting rampage on May 20, 2014, at the UC Santa Barbara campus and community after several years of methodical planning. Although he did not have the "face of rage" in the video he posted the day prior to the shooting (podcast audio, http://www.youtube.com/watch?v=5EVEq-NikxA), he clearly states his rationale for the murders he is about to commit. The day of the shootings, he was likely in a state of rage; for example, even though he had high-powered rifles, his first act was to stab his three roommates to death. He then went on a shooting spree throughout the campus, killing six more people.

Not all terrorists, even suicide terrorists, will be enraged. Some have been methodically planning and rehearsing the attack, and on the day of the event, they will be calm and cool as they approach the target. Others

may even laugh or show joy once the event begins. Religious terrorists likely believe their reward in heaven is just seconds away, sometimes causing a state of euphoria. However, in the case of an enraged opportunist, such as the white supremacist shootings at the Holocaust museum in Washington, DC, and the Jewish center in Kansas City, Kansas, the individual is pushed over the brink by some environmental factor and moves quickly to the execution stage. Or maybe there is no exact plan, but a church, school, college campus, hotel, or concert event provides the venue for the rage attack. In any case, recognizing the face of rage is important for response. Engaging enraged persons is extremely dangerous and you are unlikely to be successful either talking them down or changing their intention.

As we say in the military, the human is the best weapon system. After reflective thought on steady-state and crisis leadership, honing intuition, training, and comprehending the general types of threats and possible avenues of response, you are ready to build your organization's plan to detect, deter, mitigate, and respond to the threat.

REFERENCES

Al Arabiya News. "Black Death Kills 40 Al-Qaeda Fighters in Algeria." http://www.alarabiya.net/articles/2009/01/20/64603.html (2009).

Boureston, Jack. "Assessing Al Qaeda's WMD Capabilities." *Strategic Insights, Naval Postgraduate School* 1, no. 7 (September 2002).

Bunn, Matthew and Scott D. Sagan "A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes." *American Academy of Arts and Sciences* (2014).

Carpenter, Scott. *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy.* Annapolis, MD: Naval Institute Press, 2007.

Catrantzos, Nick. *Managing the Insider Threat. No Dark Corners*. Boca Raton, FL: CRC Press, 2012.

Catrantzos, Nick. "No Dark Corners: A Different Answer to Insider Threats." *Homeland Security Affairs Journal* VI no. 2 (May, 2010).

Commission on the Prevention of WMD Proliferation and Terrorism. "World at Risk: Report of the Commission on the Prevention of WMD Proliferation and Terrorism." (2008).

Committee on Homeland Security and Governmental Affairs. "Ten Years after 9/11 and the Anthrax Attacks: Protecting against Biological Threats," October 18, 2011.

Eckman, Paul. *Unmasking the Face*. Malor Books, 2003.

FBI (Federal Bureau of Investigation). "Weapons of Mass Destruction." (2012).

Gips, Michael A. "Secondary Devices a Primary Concern." *Security Management* 47, no. 7: 2003.

"International Humanitarian Law—Treaties & Documents." http://www.icrc.org/ihl.nsf/WebART/470-750065?OpenDocument (2014).

Kennedy, Daniel B. "A Précis of Suicide Terrorism." *Journal of Homeland Security and Emergency Management* 3, no. 4: 2006

NELP (National Employment Law Project). "Ban the Box."

New America Foundation. "Non-Jihadist Cases, 2001–2011." http://homegrown.newamerica.net/nonjihadist (2012a).

———. "Right- and Left-Wing Terrorism since 9/11." http://homegrown.newamerica.net/overview_nonjihadists (2012b).

Office of Naval Research. "Basic Research Challenge—Enhancing Intuitive Decision Making through Implicit Learning." (2014).

Rodger, Elliott. "Retribution." Video posted on YouTube day prior to massacre. Podcast audio. http://www.youtube.com/watch?v=5EVEq-NikxA

Rozin, Michael. "Suspicion Indicators Recognition & Assessment (Sira) Training." http://rozinconsulting.com/

Snow, Jon. "Sri Lanka's Killing Fields." United Kingdom: BBC, 2011.

UN (United Nations). "Report of the Secretary-General's Panel of Experts on Accountability in Sri Lanka." (2011).

Whetstone, Douglas. "'Catch the Lie': Importance of Body Language Deception Detection for Security Officials." Whetstone Security Group, Inc., 2014.

CHAPTER 9

Deterring and Mitigating Attack

> The supreme art of war is to subdue the enemy without fighting.
>
> —**Sun Tzu**

INTRODUCTION

The goal of soft target hardening is simple: Deter any would-be attackers through the presence of a secure facility and if they breach your access points or strike from inside, engage with the ability to mitigate the attack and save the lives of your staff and occupants. As discussed in Chapter 2, hardening begins with you: the acceptance the threat exists and your operation and facilities are vulnerable. You likely have taken on some amount of risk by not being able to expend the resources to protect the operation fully, whether due to insufficient resources, lack of support from your leadership, or for business-related reasons. However, there is a spectrum of hardening actions you can take from nothing to everything, from inexpensive to exorbitantly expensive. The key is to understand the desired effect and plan to use your resources in the best possible manner to lower your risk.

DHS's "Soft Targets Awareness Course" (DHS 2008) is a great place to start grasping the overview of the threat and your vulnerabilities. The four-hour curriculum provides facility managers, supervisors, and security and safety personnel with baseline terrorism awareness, prevention, and protection information. The course enhances individual and organizational security awareness and participants gain insight as to why it is important to engage in proactive security measures and define their roles in deterring and detecting terrorist activity, and defending their facilities from it. The class is held all over the country and administered by qualified contractors.

Although your security plan should be an all-hazards approach, meaning that it is suitable no matter the emergency situation, you should focus on preparedness, rather than the specific kinds of weapons or tactics the

bad actor may bring to your facility. With this in mind, you should first assess your vulnerabilities. Prior to creating or improving upon your security plan, complete the FBI's Vulnerability Assessment in Appendix C. Note that this document must be safeguarded because it spells out all of your vulnerabilities. If the total score for the organization exceeds 256, and if local law enforcement has not been involved in the assessment, notify them at once. Hand carry the document, do not email or send through a postal service. After you identify and think through your vulnerabilities, you can create a plan to reduce risk in your operation. Trust me when I say, as the officer who was responsible for the security of Air Force One and the President of the United States while he transited our base at Andrews, you cannot have too much security when faced with an unknown threat and an actor who will engage on the day and in the manner of choosing.

EFFECTS-BASED HARDENING (EBH)

We simply cannot apply all resources toward all threats; a methodology is necessary to ensure actions and resources are directed in the most effective manner to cover your vulnerabilities against the threat and lower your risk. Prior to Operation Desert Storm, the Air Force's aerial campaign strategy was that of attrition—to bomb targets repeatedly and shoot down as many aircraft as possible until the enemy lost either the will or the firepower to fight. However, in order to prosecute the war against Iraq successfully, with restraint to spare civilians and not destroy the infrastructure of Baghdad, Air Force strategic thinkers devised a new approach: effects-based operations (EBO). An EBO approach is one where "operations against enemy systems are planned, executed, and assessed in order to achieve specific effects that contribute directly to desired military and political outcomes" (Carpenter 2004). EBO provides a strategy for the application of resources, phased in a particular way to achieve the desired cumulative effect. For instance, on the first night of the war, F-117A stealth aircraft (my unit) went into Baghdad and selectively destroyed communication towers and antiaircraft batteries. Later in the war, after the battlefield was "softened," targets shifted to military headquarters and enemy airfields.

EBO provides a good theoretical foundation for our efforts to harden soft targets, and for these purposes we call it EBH—effects-based hardening. This proposes a new (or improved) way of thinking and a specific process on both physical and psychological planes. Several axioms must be accepted prior to implementing this approach:

- Actions cause results.
- Inaction also causes results.
- Not seen does not mean not there.

- The goal is to remove the enemy from the fight before it starts.
- Actions are not universally applicable and must be tailored to your situation.
- The plan is fluid; you must constantly assess and adjust based on changes in the environment.
- The "fog of war" means you do not know everything about the threat; there are inescapable unknowables.
- You have no experience with the situation that might occur in your organization; nothing that happened in the past can prepare you.

EBH provides a system for visualizing violent scenarios that might happen to your organization in an unemotional, data-driven way. In order to identify the Achilles heel discussed in Chapter 8 and other vulnerabilities that increase your risk and susceptibility to attack, you have to "go there" and visualize and map out the worst possible scenario in your facility. At the least, consider an enraged outsider, a plotting insider, an active shooter, and a kidnapping and hostage situation.

The good news is that you are fighting this "battle" on your own territory. No one knows the vulnerabilities and strengths of your operation better than you; this puts you in the position of power over bad actors when it comes to deterring or mitigating their attacks. No matter how much preplanning or surveillance takes place, or even if you face an insider threat, you have the upper hand. Accordingly, keep certain details about your plan close, think of your employees' "need to know," and draw a diagram of concentric circles with the critical operations and people at the center and continue outward to the periphery, where you may have building custodial staff and volunteers. They need security and response training, but do not need to understand the security apparatus in place or your plan for protecting the facility and its occupants.

There is an art and science to security. The science part is physical: barricades at certain locations, walk-through metal detectors to keep out weapons, and security personnel stationed at entrance points for presence. The art is using your resources efficiently and effectively to achieve strategic security objectives. EBH can complement (or replace) your current efforts. Any new security processes should be incrementally phased in to shape the behavior of your people (and the enemy), perhaps in a time-phased manner or from most to least critical. However, security is not just a program; it must infiltrate everyday operations and decision making. By baking security into the organization and not just leaving it to the security guard at the front door, you tap the full spectrum of your assets: people, equipment, and building location. You may never know what types of terrorists or violent criminal acts you have thwarted using this methodology, but at the very least you will have a data-driven plan that effectively uses your resources to cover vulnerabilities.

Move forward *unapologetically* with your security plan. Leaders at soft target locations have confided to me their sense of regret about how efforts to tighten security inconvenience their staff and visitors. Those operating a for-profit operation are often concerned with customer satisfaction and whether measures will drive patrons away. I tell them to imagine, for a second, a horrendous attack at their facility. It could be an angry ex-spouse exacting revenge, a fired employee, a disturbed teenager, or a terrorist or group seeking to make the news and further their religious or political cause. As the leader or head of security, you must face the devastated family members and explain how you failed to protect their loved ones. Being a leader means taking responsibility, not only for the good things that happen at your place of work, but also for the bad, and the very, very bad.

EBH, by its very nature, encourages the harmonizing and synchronizing of actions. For example, during an active-shooter event, the front office has a plan: one predesignated person calls 9/11, one makes an announcement on the loudspeaker, and one locks and barricades the door. These types of actions take training and practice. Similar to pilots who are thrown impossible situations to handle in the flight simulator, if you practice for the worst possible scenario, small security issues will be handled effortlessly by the staff, working together as a team. They will also be confident of their ability to handle a large-scale emergency, and this confidence makes them force multipliers to you and your security team.

Matrixing your vulnerabilities, desired effects, the means to lessen your vulnerability, and the capabilities you have and need helps with the decision-making process. Figure 9.1 is an example of an EBH decision matrix for a church or school.

How do you know if your EBH efforts are working? You can test your system by having an outside security company do a red teaming exercise on your property, a tactic addressed later in the chapter. Also, you should ask the people who work in and use your facilities if they feel safe and if not, how you could do better. Not only will you glean valuable information, but the mere process of asking for and then acting on their ideas will strengthen your relationship and open the lines of communication about vulnerabilities.

The rest of the chapter is devoted to best practices and ideas harvested from industry experts—information to guide your EBH efforts.

PHYSICAL SECURITY

(Thank you to Brian Gallagher, former physical security specialist at the US Secret Service and owner of Security at Church (www.securityatchurch.com) for assistance with the following section.)

Prioritized Scenario	Desired Effect	Means	Capabilities and Cost	Implement/Partially Implement/ Table
1. Highly visible location on busy highway draws opportunists	Lower "heat"	Remove external signage facing road	In house, volunteers, free	Implement
2. Too many people with keys to the main door	Restrict building access	Install electronic key lock on main door and obtain keying equipment and cards	Contracted; $3,000	Partially implement; rekey current lock, reissue keys; budget electronic key system for summer 2015
3. Holding meetings after hours for outside groups, attendees wandering in building	Restrict access to the rest of the building	Install locking door between basement and upstairs offices	Contracted; $1,500 with labor	Implement

FIGURE 9.1 Effects-based hardening matrix.

We cannot easily interview terrorists or those who perpetrate violent crimes about deterrents to their activity; however, convicted thieves are accessible and give valuable insight. The chart in Figure 9.2 shows responses from 360 burglars regarding physical security measures that serve as the biggest deterrents to their activities.

Note the presence of people is the number one deterrent, followed by an officer nearby (which may be substituted at night by a preparked patrol car). Alarms are effective, as well as surveillance cameras, dogs, and steel bars on windows. The limited escape route is something to consider as well.

The exterior of your building, the grounds, and the parking lot are all critical to the security of your occupants. As previously discussed, lowering the profile of your building with less signage will deter opportunists from attacking your church or school. Physical hardening of your property could be as simple as installing a security fence or raising the height of current fencing to conceal your building and its occupants (such as children in a schoolyard) and to keep out intruders. Always check the perimeter fence for breaches or the stacking of wood or objects that could allow someone to climb over the fence. Industry experts recommend the following fence standard: seven feet high, with three strands of barbed wire, six inches apart. Shrubbery should be no higher than three feet, and set back one yard from buildings, and tree branches trimmed eight feet above the ground. Outdoor lighting not only illuminating

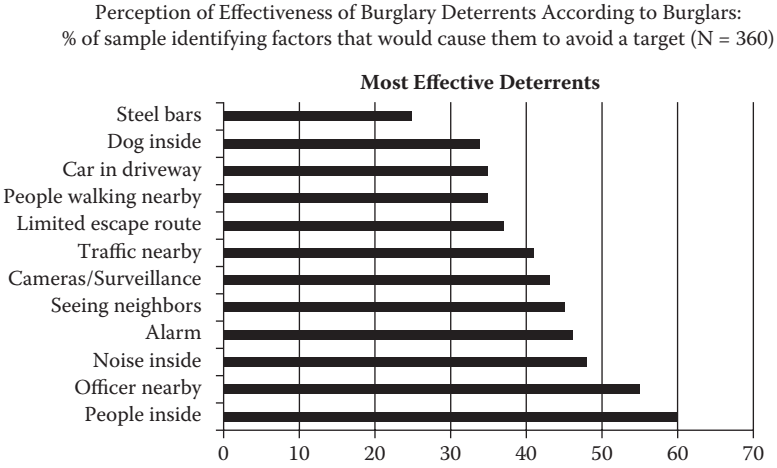


FIGURE 9.2 Most effective deterrents to burglary. (Kuhns, Kristie R., and Blevins, Joseph B. "Understanding Decisions to Burglarize from the Offender's Perspective." The University of North Carolina at Charlotte Department of Criminal Justice & Criminology. 2013. With permission.)

buildings, but also the surrounding property, is important to deter trespassers. Motion lights will keep your electricity bill lower and startle any would-be intruder. There are industry standards for external security lighting; see IESNA, ASNI and OSHA guidelines online.

Parking Lots

As illustrated in previous case studies, several international and domestic terrorists used parking lots to plant the primary bomb, stage a shooting, or place secondary devices aimed at injuring response personnel and evacuees. Therefore, you must secure your parking lot as an extension of your building. The preferable situation is to have the parking lot located inside the fence line, with a greeting area/entry point to control visitors. Churches are especially vulnerable to burglary, with service times posted outside on signage and a lot full of unattended vehicles for an hour or more. A roving parking lot security team provides an extra layer of protection.

Operations with large parking lots such as megachurches, large schools, malls, and sports and recreational venues might consider training for parking attendants called "First Observer" (http://www.parking.org/professional-development/first-observer-program.aspx). The program is jointly operated by the Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) to train parking attendants to identify a potential threat. The program also educates the parking attendants with background information on terrorist groups, their tactics, and trends as well as an understanding of weapons. Training of this type turns a parking attendant into a force multiplier for your organization.

Pre-positioned Vehicle

Perhaps you could ask your local police department for a marked police cruiser to be placed at the entrance of your building. You could offer parking to an officer who could leave his or her personal vehicle at your facility and swap out with the cruiser when off duty. The marked vehicle serves as a visual deterrent for those who might be performing surveillance on the facility. If the marked cruiser is not possible, perhaps a member of your church, school, hospital, or organization will give up an old SUV or truck, which you can mark to look like a security vehicle from afar using fluorescent tape and other tools (Figure 9.3).

There are no data to prove the pre-positioning of law enforcement vehicles deters attack; however, anecdotal stories support the theory. For instance, there is reason to suggest that Sandy Hook Elementary School

FIGURE 9.3 SUV repurposed as a mock security vehicle at a compound in the Middle East.

shooter Adam Lanza's initial target was actually Newtown High School. According to a source familiar with the investigation, Lanza's car was identified on the school surveillance footage circling the school parking lot. The official believed Lanza saw two police cars parked in the lot and decided to move on (Lysiak 2013). The absence of such procedures has been used in several "negligent security" lawsuits; for instance, in 2007, a man was killed by a shooter with an AK-47 in a case of mistaken identity in a Waffle House parking lot in Pensacola, Florida, at 3:30 a.m. In the successful lawsuit filed by the family: "The plaintiff alleged that the restaurant was located in a high crime area. The plaintiff's security experts opined that the defendant was negligent in failing to have an armed, uniformed sheriff's officer on the premises with a marked police car which would have deterred the crime" (Rose, Vangura, and Levin 2009).

If your facility is hosting a special guest—one that has been advertised to the public and may be controversial or draw protest, or even a popular celebrity—know that a bull's-eye has just been painted on your facility. You should pre-position an escape vehicle near an emergency exit closest to the place where the person is addressing the crowd. A member of your staff or a trusted volunteer should be positioned at the vehicle as the driver in case of emergency.

Traffic Duty

Soft target facilities have predictable schedules: schools have drop off/pick up, church services start and end at the same time every week, sporting and recreational events have traffic issues at the beginning and end of events, and malls are typically their busiest on Friday and Saturday nights. Choke points outside your facility present a security hazard and you need to keep traffic moving. Mir Aimal Kansi, a Pakistani citizen residing in the United States with phony immigration papers and a forged green card, became enraged while watching CNN news coverage of US operations in Iraq and CIA involvement in Muslim countries. A courier, he often drove by the entrance to CIA headquarters, noting the two lanes of traffic waiting at the light to turn left onto the agency's ground. At 8:00 a.m. on January 25, 1993, Kansi drove his courier vehicle to that very spot, emerged from his vehicle with an AK-47 semiautomatic rifle, and walked up and down the lines of vehicles, firing a total of 10 rounds, killing two CIA employees, and injuring three others. Kansi escaped the country and was arrested by FBI agents in Pakistan in 1997; he was convicted and sentenced to death by lethal injection, which was accomplished in 2002. The military actively tries to avoid chokepoints, such as long traffic lines at gates, where people are vulnerable to attack and are blocking emergency response vehicles, if required.

Many states and counties require some sort of intersection control for larger churches, schools, and sports and recreation events. Although it is tempting simply to use volunteers with reflective vests, it is important to have a uniformed police officer directing traffic along with a marked vehicle with flashing lights, not only to slow vehicles but also to show presence to any opportunist who may decide to strike during the congested, chaotic time. A possible solution is to use a member of your church congregation or the spouse of one of your school, hospital, or sports/recreation venue employees who happens to be a law enforcement officer. However, if you have to hire an officer, go directly through the county or local police departments instead of using a contractor, which is more costly and will likely outsource to the same organization.

SECURITY

We accomplish three goals through robust physical security features: portray to would-be bad actors that the facility is hardened and deter their actions, protect our property and its occupants in the event of penetration or attack, and make them feel safe, improving staff productivity and providing a better experience for users whether learning, worshipping,

or healing. In for-profit organizations, a strong security infrastructure and program will positively affect your bottom line, especially for customers who make decisions about what sporting and recreational venues they will entrust with their lives and those of family members.

Locks

Some facilities have only a few doors and others have many; no matter your situation, know that locks are critical to securing your property. Locks can be very easy to defeat if they are not made or installed properly. For instance, most locks installed on home doors can be defeated in a matter of minutes by someone with basic knowledge, which can be easily gleaned from the Internet. A simple padlock can be cut with a bolt cutter. A file cabinet can be breached by a crowbar. So how do you keep out those with bad intentions?

Although we want the visitor's first impression of the facility to be favorable, always choose security over aesthetics. Exterior doors must have, at the least, a dead bolt and never contain glass or be surrounded by glass window panes. In the Newtown, Connecticut, shooting at Sandy Hook Elementary School, the school's security procedures had just changed, requiring visitors to be admitted individually through a set of security doors after visual and identification review by video monitor. Doors to the school were locked at 9:30 a.m. after morning arrivals. Adam Lanza arrived at the school at 9:35 a.m. and the door was locked. He simply shot through the glass panel next to the door and stepped inside the school (Figure 9.4). According to the official report: "The doors to the school were locked, as they customarily were at this time, the school day having already begun. The shooter proceeded to shoot his way into the school building through the plate glass window to the right of the front lobby doors" (Office of the State's Attorney Judicial District of Danbury 2013).

Once inside the school, Lanza had a distinct advantage because he had attended Sandy Hook and had intimate knowledge of the inside of the building. However, there were infrastructure weaknesses detailed in the Newtown report, disadvantages that allowed Lanza to kill twenty innocent children and six teachers and staff members in just five minutes before turning the gun on himself when the police arrived. For instance, the report discusses the office and classroom doors: "The doors in the hallway all locked from the outside with a key. The interior door handles had no locking mechanism. All of the doors opened outwardly toward the hallway. All doors were solid wood with a circular window in the upper half of the door." Although investigators did not discuss how these doors failed to protect the building occupants, the report is replete

FIGURE 9.4 Front entrance of Sandy Hook Elementary School.

with examples of how Lanza was walking up and down the hallway trying doors and looking through windows. Perhaps, if the doors also locked from the inside, with a double key lock, lives may have been spared. Also, having windows on the doors provides visual advantage to the shooter and another way to get through the door if it is locked from the inside. Photographs taken at the scene show the classroom windows were the type that opened up and inward just a few inches, with not enough space for a child to escape. The classrooms were on the first floor and perhaps people could have fled the scene through the windows if they slid on a track. The Sandyhook tragedy gives much to consider when assessing external and internal building security.

Who has access to your building? How many people have keys to your building? Do they all need a key to the front door? Typically, too many people have keys to a building. Keys should be numbered, issued by signature, and stamped "do not duplicate." The types of locks are also important; for instance, a standard lock has a cylinder inside with a series of pins that move up and down. When you insert a key into the cylinder, it moves the pins up and down vertically; when the pins line up correctly, the cylinder rotates and the lock opens. Locks with more pins are harder to defeat; for instance, a filing cabinet lock may have three pins whereas the lock on your front door may have six or more. The depth of the pins also helps make the lock more secure, to prevent opening by mere jiggling of the cylinder using a pin. Professional locks have pins that are not merely vertical, making them extremely difficult to defeat.

Locks can also have "smart cards" or electronic chips in the key, allowing for remote access and the ability to activate or deactivate a key and to control and track access to a room. For example, using keys and locks with electronic chips allows the facility manager to give access only on certain days (church services or school days). Naturally, we should not assume people with keys to our facility have bad intentions; however, keys are routinely stolen or lost. In government facilities, lost keys often mean locks must be changed and new keys issued. Electronic keying allows for instantaneous changes that immediately prevent access in the case of nefarious intent by a thief or a person finding a lost key. The basic principle is to limit access.

Interior doors should have locks, including supply closets, which are notorious hiding places for a bad actor and/or the stockpiling of supplies for an operation. Business offices must be further hardened to protect not only from the theft of private information, but also the occupants who might be the target of a criminal act or an attack. Keys to these doors must be strictly kept to those who need daily access. Although some large hospitals now have sophisticated systems that automatically lock all doors and stop elevators in the case of a lockdown, consult with law enforcement and fire officials prior to installing such a system, as it could trap people trying to flee.

Alarms

What is the backup plan if your key system is defeated? Some soft target facilities have sophisticated alarm systems and others have none. If you do not have an alarm system, why not? Security companies can install alarm systems at your facility for minimal cost and charge modest monthly monitoring fees. If you do have an alarm system, is it the right one and are all of your bases covered? It may be time for a security assessment and upgrade.

An alarm system obviously protects your building and its occupants, but acts as a powerful deterrent to many would-be intruders. When 422 convicted burglars were surveyed, approximately 83 percent of the offenders said they would attempt to determine if an alarm were present before the burglary and about 73 percent said they would seek an alternative target if so. Among those who discovered the presence of an alarm while attempting a burglary, half reported they would discontinue the attempt, and another 37 percent said they would leave the property. About one-third of the respondents planned their crime; the rest were opportunists, mostly looking for money or drugs (Kuhns and Blevins 2013).

If you have a central alarm system, it can be wired or wireless. It can be monitored by a central location or "bells only" in which you hope the

loud alarm is a deterrent to the penetrator, who then departs the property. Remember that the alarm code is just as valuable as the master key and you should try to limit distribution of this code to staff who come to work early to open the building and stay late to close, or those who need to enter at odd hours. However, all staff should have the silent duress code number they can punch into a panel, alerting the alarm company to call law enforcement, a feature only possible with monitored systems.

If you choose a monitored alarm system, sensors will be placed on doors and windows. You may also add motion sensors to catch movement in the building and glass breakage detectors on sliding doors. When triggered, the alarm signal travels via a telephone or Internet line to a central monitoring location where an employee receives information such as your address and possibly a schematic of your building with the exact location of the breach. The alarm company will have several contacts on file and will first call you before calling law enforcement, to prevent false alarms. Typically, you will have a prearranged, easy to remember telephone password confirming your identity. You must think redundancy when deciding on an alarm system for your facility; if the person is hiding inside the building when you lock up for the day, the motion sensor will detect him or her. If the intruder can breach the external door lock and alarm (pressure pads are easy to defeat, magnetic pads, not so easy)—again, the motion sensor will work. Glass breakage detectors are important on sliding doors, as the actor may try to avoid the sensor on the track by entering through the broken glass.

As previously mentioned, if your system is monitored, an employee can enter a duress code into the panel to alert authorities; in this case, no calls will be made to protect those in the situation and law enforcement will immediately respond to the location. Also, panels typically have hot buttons to push for medical help, fire, and police; these are timesavers during an emergency. An alarm system is a great investment and most insurance companies offer discounts for their use.

You should also have a panic alarm built into the reception area; this is a simple button located under the desk that can be discreetly pushed in the event of an emergency to signal silently for help. The signal can be set up in different ways; it can be wired so the duress call will go straight to the local alarm company, which will immediately send the police. Churches, schools, and hospitals should consider having a duress button in areas where counseling takes place and possibly also in conference rooms. The panic signal button does not have to be programmed to notify the local alarm company or police department; it is possible to have it signal for backup: for a colleague to come to the area and provide backup. The button should be pushed only in a situation where there is the danger of physical violence; the staff could be trained not to enact the duress signal if someone is merely acting demanding or overly

emotional. Banks are served very well by these silent alarms, with police typically arriving while the robbery is being committed or shortly thereafter. Naturally, bank robbers know banks have these alarms and yet are undeterred. Similarly, we need to realize that security features will not keep determined bad actors from engaging.

Visitor Access and Badges

Having a solid visitor management program to control access to your facility is incredibly important. If there are several access points to the building, have clearly marked signage funneling visitors through one set of doors. Have the visitor sign a log with name, time, and cell phone number and produce photo identification for entry, preferably a government-issued card such as a driver's license. You may hold this identification in exchange for a visitor's badge. Many secure government buildings such as the Pentagon require two forms of government-issued photo identification. The best practice is to have the visitor wait in a designated area while you contact the individual he or she came to see; do not let him or her wander aimlessly around the building. Having positive control of the visitor is important. Secure schools do not let parents walk items to classrooms (forgotten lunches, books, musical instruments); they may leave the items in a designated area in the front hallway and the child comes later to collect. Sign-in logs must be kept for a designated period of time, as they will provide evidence if the visitor commits a crime on the property, is in a parental custody battle, and so forth. The rosters also allow other due-diligence activities, such as running the name through the sex offender database. Although these activities may feel uncomfortable or intrusive, remember you are responsible for the protection of hundreds, if not thousands, of innocent people. Inconveniencing a visitor is a small price to pay.

Closed Circuit Television (CCTV)

We have already discussed cameras in terms of violent criminals, who barely see them as a deterrent, hoping they aren't taping or their image is obscured enough to cause doubt of their identity. On the other hand, over forty percent of convicted burglars indicated that the presence of surveillance cameras would deter them from a target. We have discussed how some terrorists often conduct surveillance of their targets while planning, while others simply hit a target of opportunity. A key tenet of this book is that facility owners should not base hardening activities on guesses as to who might attack or how. Therefore, my opinion is that all soft target locations should have CCTV that is preferably monitored, but

at the least, is taping for later reference or evidentiary purposes. Many systems refresh on a cycle; 48 hours is probably a good point to start taping over old data. CCTV acts as a set of eyes when people are not available, and it helps gain convictions and even win court cases for you and your insurance company in the event of a lawsuit or claim.

Admittedly, CCTV does not deter a suicide terrorist who plans to lose his or her life or an enraged violent criminal who is not thinking rationally. However, if the actor believes the cameras are being monitored, they know there will be an immediate law enforcement response, compressing the timetable for the criminal act. Camera systems should be used to watch not only the front door, but also other exterior doors, hallways, classrooms and other multipurpose rooms, and the parking lot. There are state laws against filming in certain areas such as bathrooms, locker rooms, changing areas, or nursing mothers' rooms. New camera systems transmit images over the Internet, so you can watch the feed from your computer or even wireless devices such as a Blackberry or an iPhone. Another great feature of CCTV systems is pan, tilt, and zoom (PTZ) cameras that can be remotely controlled if you need to get a closer look at an individual. For outside cameras, you could also employ infrared (IR) technology to see better in the dark; in fact, many companies are now installing IR cameras indoors to capture criminal activity that may be occurring in dark corners or with flashlights. Many systems may be purchased over the counter and installed by the user; however, security system companies would be happy to bring their experts to your property to discuss CCTV coverage.

Public Address System

I strongly recommend facilities have a public address system for broadcasting emergency information to the entire building. During the Sandy Hook Elementary shooting event, one of the injured staff members unknowingly tripped the loudspeaker system when dialing 911 for help. Her phone conversations were heard throughout the building, as were the gunshots in the front office area. This alerted the teachers and staff to the crisis and they had precious seconds to lock doors and hide students. The librarian called the front office and the staff to see what was happening and the staff member told her there was a shooter; again, this was broadcast to the entire school.

The Winnenden School, located in southwestern Germany, was the scene of a mass shooting when former student Tim Kretschmer entered the school with semiautomatic weapons on the morning of March 11, 2009. Immediately following the start of the attack, the school's headmaster broadcast a coded announcement saying "Mrs. Koma is coming," which is the word "amok" spelled backward. The message was a

safety measure installed to alert the teachers of a school shooting and give them a chance to help students escape or shelter in place; it was established in Germany after a previous school massacre at Erfurt.

Intercom systems are also excellent ways to transmit specific threat and emergency information immediately. Hospitals have elaborate code systems that would be easy to adapt to other situations; for instance:

1. Code blue/code 99: CPR team
2. Code red/red alert/Dr. Firestone: fire alarm, activate department fire protocol (close fire doors, move people past fire zones, evacuate if ordered)
3. Code orange/code purple/code silver: internal incident (psychiatric patient missing, active shooter in building, active bomb threat, etc; activate case-specific disaster plans)
4. Code black/code yellow/code 10: external incident (natural or man-made disaster, mass casualties; activate department disaster plan)
5. Code pink/code Adam/Amber alert: missing infant/child (lock down all exits, be on lookout for suspicious persons)
6. Code green/code 00/all clear: all clear, resume normal duties

In one school district, a "code 303 meeting" was known universally, even among the students, as the code for a bomb threat. "Mr. Falkes" and his parents being in the office meant a bomb threat, "Professor Norris" needing to meet his wife in the teacher's lobby meant weapon/stranger on site, and an "ROTC Club meeting" being canceled meant something very bad was happening that required immediate staff-wide attention (via e-mail or intercom). At an exhibition center in London, loudspeaker calls include, "Will Mr. Goodfellow report to the security suite"—the code for a fire. A report that, "Mr. Goodfellow has left the building" is all-clear code for the fire situation. "Staff call 100" is the code for a bomb threat, and, "Staff call 100 has been canceled," is the code for the bomb threat passing. At one college, instructors use a phone code to alert security that a student they are meeting in private may turn violent. If they want a security guard to come to the office as a precaution, they call the outer office and say "I'll be a little late for our meeting with 'Dr. Barry'"; if they want a guard to come in immediately, they say the appointment needs to be postponed.

The combination of the intercom and a code system can save lives.

Ventilation System

We discussed the threat of weapons of mass destruction (WMDs) in the previous chapter and, for closed buildings and venues, it is important to

understand your central air conditioning and ventilation systems. For example, find out if your building has fresh air intakes or recycled air intakes; newer systems are likely a combination of both. Are the units located on the roof, where they may be harder to reach (ideal) or are they on the ground and easily accessible? If an attacker is using a chemical or biological weapon against the property, he or she will likely introduce it through the intake system for maximum dispersal in the building. Even over-the-counter pepper spray will affect building occupants if introduced this way. If the unit is on the roof, make sure hatches are padlocked. If the unit is on the ground, consider building a fence around the unit with a lock on the gate. If possible, try to monitor these locations with security cameras and, if your organization cannot afford security cameras, then include these locations in a walk-through for your security team or administrative staff.

Dining Halls

For facilities with kitchens, consider whether you have a "clean" environment; for instance, when they are not in use, do you secure items that could be used as weapons such as large knives? Are food items secured in tamper-proof containers or locked refrigerators so a bacterial agent cannot be introduced? In churches, kitchens may only be used once a week, so they may be a good place for an insider or potential attacker to store supplies. Dining halls are particularly vulnerable to a mass shooting or kidnapping/hostage situation because there can be many people in a confined space; several attacks already profiled in this book have occurred in a cafeteria.

EMERGENCY PREPARATIONS

Hardening your facility includes being prepared for any contingency, whether there is an emergency in your town or city and you are receiving scared or hurt people, or whether you have a security incident on your property and need to provide medical care and possibly shelter in place until help can get to you. The first action is to take the applicable free FEMA courses listed in Appendix B, such as IS-360: "Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship" or IS-362.a, "Multi-Hazard Emergency Planning for Schools."

Specifically, you should have a four-pronged approach to cover all bases: a "hold room" to secure your leadership, a command center for

you and your key staff, a strong medical program, and the ability to shelter in place.

Hold Room

A hold room is a place where you and other key staff or important visitors can retreat in the event of an emergency and hold for an undetermined amount of time. The room should be located in an evacuation area or point of the building where law enforcement can most easily get to you and you can get out as needed. The hold room can be as simple as a room with a door and lock or as elaborate as an underground facility. It may be worth the money to purchase a security door for the hold room—whether an "intruder" door that will resist being breached or a ballistic door that protects from forced entry but also repels 30.06 caliber rounds. At the very least, you want to make sure that the door can lock from the inside and it has no windows. Although it seems counterintuitive, it is best to select a room with no exterior windows for additional security. The hold room must have a landline phone in case cellular service is not working, and you may also want to have a charged cell phone in the room in the event the phone lines are not working. Also pre-position a case of water and energy bars in case you need to sustain those in the hold room for more than a few hours. Flashlights are also a good idea in case the electricity goes out, as well as a battery-powered radio so you can get news updates on the unfolding situation. The goal in an emergency is to get out of the facility; however, if that is not possible, the hold room will buy you time until law enforcement arrives. Be sure to add checking the hold room phones, supplies, and door lock mechanism to your facility walk-through checklist.

Emergency Response Team and the Command Center

In the event of a major incident in the surrounding community or at your facility, you may want to stand up an emergency response team and have an area that can serve as your command center. The command center might be the same as the hold room. You will need landlines, flashlights, and a radio with extra batteries, water, and a supply of nonperishable food, such as energy bars. Handheld radios that are charged and ready are a plus if someone needs to leave and communicate with the command center. Pads of paper, pens, and even a whiteboard with dry erase markers would be helpful. This is the central repository for information and checklists.

Next, assess your potential emergency team. You may want to poll your employees to evaluate the additional skills and resources they bring to your operation. For instance, do they have a conceal carry permit and do they regularly carry a weapon? Do they have medical training, private security or a military background, or experience as a volunteer firefighter or paramedic? When formulating the emergency team, think about the skillset and also the mindset: can he or she handle an extremely upsetting, emotional event and be an asset to the team, instead of a liability? Once your emergency team is identified, create an "alert roster" with their names and cell, home, and e-mail contact information. Make sure to check the information regularly to ensure currency.

Who should be around your table? If your staff has directors or heads of specialized sections, they should each be there—security, facilities, communication, human resources, legal, etc. Also, if you have any counselors on staff, one should be designated to sit on the emergency response team. Additionally, have someone on your team in charge of handling the press and social media. If your building has been attacked or there is a mass hostage situation, others will blog, tweet, and Facebook; take control of the "message" and transmit what you want people to know about what is happening inside. Also, information you transmit could save the lives of others; for instance, during the strong earthquake on the Eastern seaboard on August 23, 2011, citizens in New York City saw the Twitter alerts about an earthquake that originated in Virginia 15–20 seconds before seismic waves struck the city. According to Facebook, the word "earthquake" appeared in the status updates of three million users within four minutes of the quake. Twitter said users were sending as many as 5,500 messages ("tweets") per second.

For the purpose of keeping control of the message and transmitting data that could warn others of danger, you may want to have Twitter and Facebook shell accounts established to use as needed. Naturally, do not transmit any information about law enforcement activity in the building—which responders are on site, numbers, and their plan. In many cases, such as the Westgate Mall siege, the terrorists are also using the media to transmit and television and radio to assess the activities of law enforcement outside. Also, never transmit the number of injured or fatalities, or any pictures that could be used as propaganda by the bad actors or disturb family members.

I recommend you have a binder with checklists for each situation that could arise. One thing you *must* have on hand are maps of the building and/or blueprints as these are critical for first responders and law enforcement, especially if there is a hostage or active shooter situation. These floor plans must have cardinal directions and specific distance by feet (and even steps); walk your buildings and grounds and then map it out. Law enforcement will want to know everything about

the ventilation system ducts, whether doors open in or out, and location of light switches. This is why you must know every single inch of your property; you will be the expert they turn to for answers.

Perhaps your binder will include checklists for different contingencies that your facility might face. The best way to ensure your team is prepared and ready to handle an emergency is to practice through exercises. Take the FEMA courses listed in Appendix B, specifically IS-120.a, "An Introduction to Exercises"; IS-130, "Exercise Evaluation and Improvement Planning"; and IS-139, "Exercise Design." In addition to full-scale practices, crisis "table top" exercises where you and the team report to the command center and simply talk through the event are also a must, perhaps quarterly. There are experts who can create scenarios tailored to your organization, or you can simply draft the scenario yourself based on past events such as the Beslan school and Moscow theater sieges, the Boston Marathon attack, Columbine, and so on. Run through it with the team and keep throwing in unexpected problems such as the phones dying, a family member breaching the cordon and entering the building looking for a loved one, or the electricity going out. Remember the "pilots-in-the-simulator" approach; make it very difficult or even impossible for your team to handle and they will rise to any future challenge and succeed. During contingency operations drills in the military, a card may be handed to the leader within the first few minutes of the exercise indicating he or she is out of the fight—either killed in the attack or otherwise incapacitated. This forces the team to consider who would step up and lead and gives the person the opportunity to sit in the "hot seat." Of course, you are not on your property 24/7, and there is a possibility a crisis will strike while you are away. Do not be the single point of failure for your team.

Something to ponder are the trigger points for action. Let us say there is an emergency in the community and it is infringing on your property, threatening your facility and the people within. When should you abandon the facility and how? I was fortunate to attend a conference session in Dubai regarding hotels in the Middle East and their contingency plans. During the 2012 uprisings in Libya, several US hotels were caught in the middle of the crisis in which a US ambassador and his team had already been killed in Benghazi and the embassy burned to the ground. One hotel unexpectedly was the recipient of an influx of people after the embassy made an announcement (without coordinating) that all Americans should go to this particular hotel. The hotel manager looked out the window and saw a line of cars and Americans outside his property's gate, which he had locked down. Naturally, he took all of the Americans in and bedded them down with the rest of the hotel customers and staff. But at some point, he had to make the difficult decision to leave the property, possibly forever because it would likely

be overrun and destroyed by militants. They needed more buses than originally planned, and people could only take one small bag, leaving the rest behind. Travel arrangements had to be made with airlines, and the now-large convoy of Americans to the airport required security. A bad situation quickly degraded to the worst scenario. Fortunately, they all made it out of the country; however, the property still sits vacant.

The manager of the hotel in Libya told us he wished that he had had three plans on the shelf that day, instead of just one. He called them the "alpha, bravo, and zulu plans," Zulu was the worst-case scenario of no rescue possibility and ditching the facility. The account of the hotel manager and others profiled in this book teaches an invaluable lesson: expect the unexpected and plan accordingly.

Bomb Threat

Organizations all over the country receive bomb threats every year by phone, mail, e-mail, or note at the facility. Most of these threats are geared toward one main purpose: to disrupt everyday activities, whether final exams, a church service, or a major event. Although many threats turn out to be benign, attention-getting mechanisms, you should not guess—call law enforcement immediately and they will conduct a thorough sweep of the building, possibly bringing dogs that can detect explosives and other high-tech equipment to ensure the building is clear. The bomb threat sheet provided in Appendix D should be close to all telephones so the call recipient can immediately write down the details from the call. Train those who answer your phones to stay calm and keep the caller on the phone as long as possible to gather information about gender, background noises, etc. The conversation might even allow your staff member to ask when the bomb will go off, to include the time and date, and to query about whether the bomb has already been placed in the building and, if so, where. Practice is key to ensuring your employees respond properly when receiving a phoned-in bomb threat. Appendix E contains the evacuation distance chart that you can use to move people, vehicles, and the like away from the location immediately. Have an evacuation plan, post it, and practice often.

Medical Program

A good medical program is an important part of your security plan. During a medical emergency, unless at a hospital, your staff, building occupants, and visitors may not be able to think clearly and respond while being part of an intensely stressful situation, such as violent

shooting. Therefore, it is important to have medical protocols in place that everyone is familiar with and to train to the worst possible scenario.

There have been cases of people freezing and being unable to dial 911. It was not because they did not know the number "911" but rather because an additional digit was needed to get an outside line, like dialing 9 first. To prevent these kinds of situations, simply place a sign or sticker on every phone that reminds the caller to dial 9 for an outside line and then 911 in the event of an emergency. Recall that part of your hardening efforts will be to ask the staff if they have special skills, including first aid, CPR, or advanced emergency medical care. During an emergency, have a plan to find these people and get them to the scene. Your organization may want to sponsor training days with on-site classes delivered by the American Red Cross, American Heart Association, or the National Safety Council. Check with your staff, church membership, and parents of your students; you may have certified trainers who can teach one of these classes. CPR training for all is a must, and your organization should also consider purchasing automated external defibrillators, known as AEDs, now located in public areas such as airports and shopping malls. These devices are used to shock a person's heart back into a healthy rhythm and are designed for the lay person who has no training, as the unit gives verbal commands to the user on how to use the apparatus. Based on the size of your facility, you may want more than one AED. Make sure you perform routine checks to ensure the battery is charged; add this to your security checklist.

There are many helpful smartphone applications on the market with CPR and tourniquet instructions that you and your staff could preload into your phone or tablet computer. I have compiled a list of emergency-related apps in Appendix F for your consideration.

A first aid station or a central repository for supplies is a good idea. Based on the size of the facility, you may want one on each floor. These range in all types of sizes, shapes, and prices. However, it is important to have at least a rudimentary first aid supply available in the event of an emergency, with many gauze pads and dressings, roller bandages, adhesive bandages including butterflies for deep cuts, tape, scissors, antibiotic and antiseptic salve, "space" blankets, and latex gloves. You may also want to have breathing barriers with one-way valves in case you need to administer CPR to multiple victims. Some kits have the equipment needed to run a peripherally inserted central catheter (PICC) line IV with fluids, as necessary. I recommend keeping these supplies packed in backpacks, as "go kits" for easy transport to the scene of the emergency. Finally, your organization should consider joining the Red Cross Ready Rating Program, which is outstanding and free. The program offers an online 123 point readiness evaluation for businesses, churches, schools, and other organizations to assess

preparedness for an emergency and help to address vulnerabilities (American Red Cross 2014).

Finally, consider purchasing hoods for your employees. A product I used extensively in the Air Force is now available for purchase by individuals and companies. The victim rescue unit (VRU) escape hood is a head and respiratory protective hood that can be donned quickly and is compact, lightweight, and totally enclosed with its own oxygen supply. The VRU will protect the user from smoke, chemicals, biological agents, and radiation. It is available for order online (http://myescapehood.com/). You may want to place hoods in your vehicles, and pre-position enough for your ERT in the command center.

Shelter in Place

During emergencies happening either outside your property or on it, you may choose to direct the staff and building occupants to "shelter in place." This term is widely used by the military and government agencies; the concept originates from procedures taken during a nuclear, chemical, or biological attack. You should prepare for this worst scenario where you need to create a barrier between yourself and potentially contaminated air outside, a process known as "sealing the room" as a matter of survival. This type of sheltering requires prior preparation, planning, and practice.

First, designate a room or rooms with the least numbers of windows, a landline phone, and are stocked with water and nonperishable food supplies such as energy bars. Have a pre-positioned emergency kit with flashlights and a battery-powered radio, and do not forget extra packs of batteries. Gather all building occupants into the room(s), bringing in your first aid backpack "go kits," and then lock the doors and close the windows and all air vents. Turn off fans, air conditioners, and forced-air heating systems. Seal all windows, doors, and air vents with thick plastic sheeting and duct tape. Consider measuring and cutting the sheeting in advance to save time; it must be wider than the opening you are trying to cover. Secure the four corners first with duct tape, pulling the sheeting tightly across the opening. Then tape down all edges to form a seal.

"Shelter in place" is now a term commonly used during active shooter or other violent situations, as a way to keep people inside locked rooms. If sheltering during a violent attack, first lock the door from the inside and cover any windows on the door. Turn off the lights. Move as much heavy furniture as you can in front of the door to prevent it from being kicked in. Move to the back of the room. Tip over long tables and hide behind them in the far corner of the room, lying flat on the ground to lower your profile. Silence all cell phones and pagers and be absolutely quiet.

If you are hit by debris or a stray bullet, do not cry out; remain as quiet as possible and play dead. For more on how to prepare your staff and building occupants for an active shooter situation, I recommend reading DHS's active shooter booklet (DHS 2014) and viewing the Houston Police Department's video "Run, Hide, Fight" (City of Houston 2013).

ELEMENTARY SCHOOLS IN FOCUS

While accomplishing research for this book, I watched video from scenes of church bombings, school stabbings and shootings, the mall massacre in Nairobi, the Moscow Theater siege, and the attack at Beslan. Although each event is disturbing and was horrific in its own way, the three-day Beslan attack was perhaps the most heinous. Schoolchildren are particularly vulnerable due to their size and inability to protect themselves, other than running fast and away from the scene, which several children in the Sandy Hook shooting were able to do. Children have more difficulty than adults discerning between real life and fiction; in the middle of a hostage situation or an active shooter event, they are likely to freeze in a state of suspended reality while trying to decide if it is a staged event or real life. A teenager or adult in today's society is more likely to realize the gravity of the situation and take some type of action to run, hide, or fight.

Therefore, I asked a colleague, Ralph Fisk, who works in the emergency management field and has experience with school preparedness, for advice regarding the challenges and tactics for hardening elementary schools. Please see the checklist in Appendix G.

In terms of school attacks, often the disgruntled actor has ranted on social media about his plight, like UC Santa Barbara shooter Elliot Rodger, who posted a long YouTube video prior to the shootings and had a 145-page manifesto detailing his disgust with his fellow college students. Social media is not only a place to rant, but an outstanding recruiting tool. A disgruntled employee who is vocal about his or her dissatisfaction with your organization makes them a target for bad actors looking for an insider to help plan an attack. Stay vigilant and monitor social media and the Internet through keyword searches to see if anyone is discussing your facility and operation.

Marisa Randazzo is a former chief research psychologist for the US Secret Service who applied a "threat assessment" model to examine the behavior of forty-one school attackers over the previous twenty-six years. She found there was no good "profile" of the type of person who becomes a school shooter. However, there were similar patterns of behavior. School shooters did not just "snap" and begin shooting impulsively; they planned. The attacker was vocal about his or her angst or intentions, trying to procure weapons, writing about the situation in journals

and schoolwork. Randazzo states that "paying attention to changes in kids' behaviors and regularly conferring with one another about smaller threats is key to heading off bigger ones." Of the shooters she profiled in the study, Randazzo found: "These are not kids who were invisible—they actually were on multiple radar screens" (Toppo 2014). In 2014, there were several cases of concerned parents and friends reporting odd and worrisome behavior to school officials and law enforcement, a practice we must encourage, even though the informant likely does not want to get involved.

As a result of the spate of school attacks in the recent year, law enforcement officials have stepped up efforts to hold active shooter drills at schools—sometimes, in a controversial move, using students as role players. On May 19, 2014, at Jefferson Middle School in Tennessee, emergency responders converged on the school after a "report" of shots fired and injuries. The school system fully participated and practiced the evacuation of hundreds of students by bus to a nearby church. Officers and paramedics had to find and subdue the shooters, as well as tend to twenty-two casualties, and school officials had to "lock down" the school and evacuate the students (Marion 2014). This type of realistic exercising is the best possible preparation for the school staff, teachers, students, and local law enforcement in the event of an active shooter situation.

HARDENING THE COLLEGE CAMPUS

Although all of the physical security procedures covered before can be applied, target hardening is not just about barricades and cameras, but also relationships, psychological preparation, and resiliency. Soft target hardening must also harness and apply the soft sciences.

Building Relationships

Several opportunities already exist for schools to partner with law enforcement to address vulnerabilities on campus and harden against threats; however, few engage. This is also a good model for other countries wishing to increase partnering activities between academia and government security organizations. The local FBI office can assist schools with points of contacts for these programs:

1. *The National Security Higher Education Advisory Board (NSEAB).* In response to increased concerns about security on college and university campuses and to open the lines of communication between academe and law enforcement, the

FBI created the NSHEAB in 2005. The NSHEAB consists of nineteen university presidents and chancellors who meet on a regular basis to discuss national security matters that intersect with higher education. Previous panels included discussion on protection of weapons of mass destruction research and laws regarding domestic terrorism investigations on campuses. A new cyber subcommittee is addressing computer vulnerabilities on campuses.

2. *The College and University Security Effort (CAUSE).* FBI special agents in charge meet with the heads of local colleges and universities to discuss national security issues and share information and ideas. CAUSE is a conduit for schools to understand how to harden against the counterintelligence threat.
3. *National Counterintelligence Working Group (NCIWG).* NCIWG was designed to establish strategic interagency partnerships at the senior executive level among the US intelligence community, academia, industry, and defense contractors.
4. *Regional Counterintelligence Working Group (RCIWG).* The RCIWG is a subset of the NCIWG and focuses on special vulnerabilities of local institutions and the threat.

Productive dialogue between education and law enforcement leadership will enhance security efforts. Colleges and universities would be better informed on the threat and mitigation opportunities and can in turn educate government security officials on the rights and protections afforded by the First Amendment in academia and the unique challenges facing our schools. In terms of procedure and policy, college administrators responsible for creating and executing human resources, training, and other programs designed to reduce vulnerability to infiltration and recruitment on campus will benefit. The dialogue will also educate legal personnel in higher education and technology transfer offices at higher education institutions responsible for the execution of sensitive government contracts. The following are suggested questions for colleges and their off-campus law enforcement counterparts:

1. What is the health of this relationship, perceived and real?
2. What is working between the two "tribes"?
3. What are the perspectives regarding which entity is ultimately responsible for protecting the higher education enterprise?
4. How do internal and external factors contribute to the relationship?
5. What policies, procedures, and training would enable a healthy partnership?
6. How can we ensure that faculty and students are part of the solution through increased awareness and decreased vulnerability?
7. How can we open the lines of communication between higher education and the intelligence community?

Students and Staff as Force Multipliers

Often, we fail to share vulnerability information with those who can help us the most: the population we serve. As previously stated in the book, civilians are now the target and therefore have the right to engage in protective activities. Rationale for withholding threat information ranges from not wanting to scare people to not making the organization's weaknesses or vulnerabilities public for business or accreditation reasons. The culture must shift to one in which having a vulnerability and threat dialogue with customers and staff is seen as a sign of strength, not weakness.

As a result of our unwillingness to convey the threat, the "see something/say something" campaigns are largely ineffective and can flood the system with useless data. If citizens do not know the specifics, we will not fully leverage this incredible tool. A better approach would be: If you see (*fill in the "what"*), you say (*fill in what data we want them to collect*) to (*agency they should contact*).

For instance, with respect to meth labs on campus, we may want town pharmacies to be cognizant of repeat pseudoephedrine buyers and give the information to a local drug task force. Agriculture schools have a special resource coveted by bomb makers: fertilizer. Therefore, they must know how to protect the material and report any theft or suspicious activities. Small local airports should be trained to recognize suspicious drug or human trafficking activities. Schools hosting sensitive government research and development (R&D) contracts should ask law enforcement experts to train professors to understand their value to countries of interest and to recognize elicitation attempts by students and report them to the local FBI office. Students participating in sensitive R&D activities, in military ROTC units, and degree programs such as criminal justice and national and homeland security might also receive specialized training to make them force multipliers on campus. The administrative staff that handles the J-1 visa process should know who to contact if a student is a no-show for classes or leaves the university. Clearly, just starting the conversation is a hardening method.

Exercising Due Diligence

If you ask a college president who is responsible for protection from foreign theft, terrorist threats, or a criminal element on campus, he or she may point toward the local police department and FBI office. If you ask law enforcement, they may point to the campus leadership. In the past, schools have very much acted like victims when a national security or major criminal incident occurs, instead of accepting any type of responsibility. When a school reports a violation of government rules

regarding R&D programs, it is typically only "slapped on the hand" and funding is not pulled. In April 2011, the FBI Counterintelligence Unit issued a white paper indicating the escalation of targeting and collection activities, asking universities to please engage to protect their programs (FBI 2011). Who is responsible for the existence of a major spy ring on a research campus, a meth lab in a dorm, or a student whose J-1 visa has expired, yet is still on campus? There is an urgent need for an honest dialogue about responsibility and establishment of punitive action against those who fail to engage properly. This could be the withdrawal of government R&D funds from a campus or a higher level government investigation into failure of local law enforcement to protect the school. As it stands, the lines of ownership are blurred—another vulnerability.

Colleges and universities are soft targets and extremely vulnerable to nefarious activities ranging from misdemeanor crimes to drug trafficking to infiltration by agents of foreign governments. As routine targets become less accessible, domestic and international terrorist groups might also prey on the open campus environment to recruit, spread propaganda, or even stage an attack. In addition to physical hardening, soft targets can be further protected by activities to educate the populace on the threat and build relationships to open lines of communication and ensure unity of effort during a crisis. The successful partnering of academia and law enforcement is essential for both to meet their critical missions. The overarching goal is a balanced and rational approach that preserves our tenets of academic freedom and accessibility yet protects colleges and universities from exploitation.

CHURCHES

All of the preceding hardening tactics certainly apply to churches. For the best example of securing worship services, we might turn to synagogues to gather their ideas and perspectives. Those of the Jewish faith have a history of persecution and Israel is actively targeted by Islamist extremists who have the stated goal of annihilating the country. Naturally, in the face of so many enemies, the Jewish people have unique concerns about securing their facilities. Many synagogues have always employed armed plainclothes security officers, who not only work the perimeter and entrances, but are also seated among the service attendees. Security was tightened with the shooting at a Jewish community center in Los Angeles in 1999, the al-Qaeda attacks of 9/11, and the shootings on July 28, 2006, by Naveed Haq, a self-proclaimed "Muslim American, angry at Israel," at the Jewish Federation office in Seattle. The attack at the Holocaust Museum in Washington, DC, on June 10, 2009, and at the Jewish Community Center in Kansas City, Missouri, on April 15, 2014,

further reinforced the need to protect those of the Jewish faith not only from radical Islamists but also American white supremacists.

The SAFE Washington program (http://www.safewashington.com/) provides an outstanding model of cooperation between religious facilities and federal, state, and local law enforcement. For its eighty Jewish entities, SAFE also "develops best practices for disaster response, community security, community preparedness, and provides low cost or no cost training for community partners through annual training." The website has a password-protected area with secure files only for SAFE members. I would hope there is some intelligence sharing and analysis between law enforcement and SAFE. An outstanding tutorial entitled "Synagogue Security: The Basics" (Moses 2014) gives five pages of security pointed at those leading or securing synagogues. Guidelines for handling visitors, suspicious packages, and security incidents are thorough and tailored to the religious environs.

Following the attack on the Sikh temple in Wisconsin in August 2010, the Sikh community also took actions to better secure their facilities. Using security "sevadars" or volunteers, the temples are protected by trained individuals and the guidelines are to "act without fear, act without anger, act to defend the weak, act to protect the innocent" (Sant Sipahi Advisory Team 2014). As with the Jewish community, much can be gleaned from the activities of those previously targeted to secure their facilities and congregations. There must be a balance between security and the open, welcoming environment that is part of religious doctrine; however, ignoring risks and vulnerabilities is not prudent in today's world.

HOSPITALS

Most hospital planning efforts are centered on response to a natural disaster or mass casualty incident in the local community. Also, there is in-depth planning and training for staff on how to react to common hospital crimes such as violent outbursts in the emergency room, attempts to steal drugs, and domestic situations with spouses and parents. OSHA 3148 requires hospitals and healthcare organizations to do annual workplace violence assessments, and more than thirty-three states also require enhanced protection of hospital and healthcare staff, typically from enraged patients.

However, depending on their operations, hospitals themselves are targets for domestic terrorists such as antiabortion and animal rights activists. Examples presented in Chapter 5 show al-Qaeda and splinter groups are actively targeting first responders at the scene of the incident and then later at the hospital when victims and family members arrive for care. After a few near-misses at its own facilities, the United Kingdom

seems to be leading research on the threat of terrorist attacks against hospitals. Recommended studies include "The Vulnerability of Public Spaces: Challenges for UK Hospitals under the 'New' Terrorist Threat" (Fischbacher-Smith and Fischbacher-Smith 2013), which started the conversation in England regarding the vulnerability of healthcare facilities.

Similar to churches, hospital culture dictates that doors are always open to the masses and restricting entry usually is not possible or desirable. Hospitals not only carry great liability for patient care but also many state patients' bill of rights/state licensing regulations direct patients "receive care in a safe environment." This naturally extends to protection from criminal and terrorist elements and attack. DHS recognizes that nonprofit soft targets such as hospitals need financial assistance to bolster their security and include money in their budget for security enhancements; however, this money is usually apportioned to the states for further dissemination. FEMA has a direct funding program through the Nonprofit Security Grant Program (NSGP). In FY 2014, NSGP was funded to $13 million and plays an important role in the implementation of the national preparedness system by supporting the development and sustainment of core capabilities.

Core capabilities are essential for the execution of each of the five mission areas outlined in the national preparedness goal. The FY 2014 NSGP's allowable costs support efforts to build and sustain core capabilities across the goal's prevention, protection, mitigation, response, and recovery mission areas (FEMA 2014). Several hospitals received NSGP grants in 2014, including John T. Mather Memorial Hospital in New York, which used $75,000 to upgrade its security system, including a new camera system and cards and a card reader for one section of the hospital. Researching how hospitals are using the NSGP grants is a good idea before applying, in order to better tailor the request and posture the hospital for success.

Emergency room entrances are not the only concern; hospital loading docks also present vulnerability. International Association for Healthcare Security and Safety President Lisa Pryse describes loading docks as "volatile" and "often overlooked" and notes there have been two instances where active shooters entered hospitals through unsecured loading dock doors (Canfield 2013). Security cameras should be installed on loading docks as an absolute minimum and a vehicular access control system is also desirable.

MALLS

Naturally, as businesses that are trying to attract customers and make a profit, malls prefer to avoid heavy-handed security measures like metal

detectors, armed guards, and bag screenings. They gravitate toward more passive measures, such as mass crowd surveillance and using human behavior theory to identify would-be troublemakers.

However, the Westgate Mall massacre served as a wake-up call to malls worldwide, which are now upgrading cameras and adding layers of security to protect their businesses and shoppers. Several lessons learned from the strategic response must be addressed in communities hosting malls. First, Kenyan officials did not act to protect their lucrative soft targets despite intelligence reporting on increased capability and threat of active, known, and capable al-Qaeda groups and chatter about their targeting of malls and other civilian venues. Therefore, the mall staff and security officers had no idea the threat was high and likely did not raise the security posture. Second, the police and military had no ability to coordinate and had never practiced communicating or working through thorny first-response issues such as who is the incident commander at a mass shooting event. This lack of coordination resulted in police being fired upon by the military while trying to rescue shoppers. Furthermore, military forces had only exercised a rescue scenario one time and this was their first real-life experience with a mass hostage situation; they were late to the fight and wholly unprepared, lacking even basic equipment such as night-vision goggles. As noted in the case study in Chapter 6, the behavior of security forces at the Westgate Mall lacked professionalism and discipline. Their rampant looting that trumped finding the terrorists prolonged the siege and exposed a degree of corruption that shocked the public and tarnished confidence in the forces' ability (and desire) to keep the population safe. There are many lessons learned from the Nairobi disaster to incorporate into our training and exercises.

In light of the Nairobi attack, several malls in the United States have held large counterterrorism and mass casualty exercises in 2014. Typically led by the FBI, these exercises happen after mall hours.

In Portland, Oregon, joint training between local law enforcement and mall personnel paid off during an active-shooter event at the Clackamas Town Center in December 2012. Responding officers knew the mall layout from the training session and were able quickly to corner and stop the shooter, who had already killed two shoppers and seriously wounded a third in a random act of violence. The training initiative is one of many positive developments driven by the International Council of Shopping Centers (ICSC), which, in conjunction with the Department of Homeland Security, Federal Bureau of Investigation, and police, dramatically improved readiness throughout the mall and shopping center industry. Mall security, formerly ridiculed and scoffed at in pop culture, is now a highly trained, professional force (Bradley 2013). They are faced with a rising number of violent incidences ranging from assault to gang violence and mass shootings and are learning and sharing best practices globally.

A new study examined the infrastructure of the Westgate Mall and how it allowed for a successful asymmetric attack by a small group of men against a large group of first responders and military personnel and apparatus. For instance, the open atrium allowed the shooters to get a high position on top floors and shoot down at fleeing customers and arriving police and military. However, the atrium also provided an advantage for store owners on top floors, some of whom could see the carnage below and were able to lower their security doors and barricade themselves in the store. Enclosed areas, such as the casino and the cinema, were used as holding areas for hostages (Butime 2014). Studying the Westgate Mall attack from the perspective of the element of surprise achieved by the attackers, the vulnerability of shoppers, the physical layout of the mall, and the poorly coordinated response is critical for all who operate, secure, and visit malls.

SPORTS AND RECREATION VENUES

As discussed in Chapter 6, sporting and recreational venues have been targeted by terrorist groups who appreciate the large, dense crowds and televised coverage that will ensure a ripple effect of fear across the populace. Current security procedures include limiting entrance points, limiting the size of bags and thoroughly searching them, and using CCTV and facial recognition technology.

Unfortunately, most venues rely on part-time, low-paid security guards who are both the first line of defense and the weakest link in the sports venue security infrastructure. In 2013, California revoked 154 security guard licenses, often due to criminal convictions discovered after the license was issued, and Florida revokes an average of more than 350 security licenses annually for criminal records. Compounding the problem, there is a "county option" approach to licensing and training of part-time security guards. States vary wildly in their procedures and seven require no security-guard licensing at all. Among those states that do, several, including Massachusetts, do not require training. In Florida and California, perhaps the strictest states, 40 hours of training are required, including a course on terrorism awareness and weapons of mass destruction. Some companies have classified employees as "event staff" in security roles at stadiums to avoid training requirements and to increase profits (Schrotenboer 2013). Also, in the quest to increase profits, sports venues often award security guard contracts to companies that are the lowest bidders. We need to remember part-time staff and volunteers provide a vulnerability in terms of facility access and the ability to stockpile supplies. They can also glean an intuitive understanding of the infrastructure and its vulnerabilities.

According to an Israeli security consultant, there is another inherent problem with security in the United States: Security personnel "don't watch the race, they watch the crowd. That's what they didn't do [at the finish line of the Boston Marathon]" (Schrotenboer 2013). The same consultant explains how, in Israel, unattended packages and backpacks are given about 10 seconds before a security official engages. The next time you attend a sporting event, look at the security guards. Are they looking up into the stadium and scrutinizing people walking by? Or are they watching the game, concert, or event? A quick Internet search yields many pictures from major sporting events such as football and baseball games where professional and volunteer security team members are facing in the wrong direction—the most distressing at the Boston Marathon finish line, seen as the first bomb exploded (Figure 9.5).

In January 2005, the Department of Homeland Security launched the first online vulnerability self-assessment tool (ViSAT) for public venues such as large stadiums. The online tool incorporates industry safety and security best practices for critical infrastructure to assist in establishing a security baseline for each facility. Modules focus on key areas such as information security, physical assets, communication security, and personnel security. As part of the National Infrastructure Protection Plan, DHS also offers site visits and other helpful assistance to partner with owners, operators, and security at commercial venues (DHS 2014). There is a delicate balance between providing security and an enjoyable experience for participants in and spectators of sports and recreation events; with technology, training, and practice, this goal is attainable.

FIGURE 9.5 CCTV capture: first bomb explodes at finish line.

RED TEAMING SOFT TARGETS

As mentioned in Chapter 2, a healthy dose of imagination is needed to protect your facility from threats and to expose your vulnerabilities. According to the 9/11 Commission Report: "It is therefore crucial to find a way of routinizing, even bureaucratizing, the exercise of imagination. Doing so requires more than finding an expert who can imagine that aircraft could be used as weapons" (National Commission on Terrorist Attacks upon the United States 2004).

Every security measure has the opportunity to work, but if it fails, it works for the offender. Unfortunately, you, as the facility manager, operator, or security professional, may not see the flaws in your security plan, or be too close to imagine how your techniques could be defeated. In order to have the best plan and make sure your methods work, you truly need to think like the bad guy. Red teaming may be an answer. The term "red team" comes from American military war gaming, where the blue team was traditionally the United States and, during the Cold War, the red team was the Soviet Union. Defined loosely, red teaming is the practice of viewing a problem from an adversary's or competitor's perspective. The goal of most red teams is to enhance decision making, either by specifying the adversary's preferences and strategies or by simply acting as a devil's advocate. Red teaming may be more or less structured, and a wide range of approaches exists. In the past several years, red teaming has been applied increasingly to issues of security, although the practice is potentially much broader.

Superior red teams tend to (Mateski 2014):

- View the problem of interest from a systems perspective.
- Shed the cultural biases of the decision maker and, as appropriate, adopt the cultural perspective of the adversary or competitor.
- Employ a multidisciplinary range of skills, talents, and methods.
- Understand how things work in the real world.
- Avoid absolute and objective explanations of behaviors, preferences, and events.
- Question everything (to include both their clients and themselves).
- Break the "rules."

A red team can undermine a decision maker's preferred strategies or call into question his or her choices, policies, and intentions. As this might be uncomfortable, it is important to put the security of the innocent people who occupy your facility ahead of any ego, sunk cost, or group think about the security of your facilities and organization.

In particular, the Homeland Security Act requires DHS to apply red team analysis to terrorist use of nuclear weapons and biological agents. As terrorists seek to exploit new vulnerabilities, it is imperative that

appropriate tools be applied to meet those threats. Therefore, most red teaming effort currently lies in the WMD spectrum, with professional teams trying to penetrate nuclear facilities, chemical and biological weapons labs, and even military installations that own or operate these sensitive activities. A red team is a group of subject matter experts (SMEs) with various appropriate backgrounds that provides an independent peer review of your processes, acts as a devil's advocate, and knowledgeably role plays the potential enemy. Red teaming can be passive and serve to help you understand the threat and expose your biases and assumptions. Or, activity can be active as the red team attempts to probe and test your security to expose your strengths and flaws. Training is another aspect of red teaming.

Although red teaming for soft targets does not exist today, I believe there can be some cross-application of methodology, currently employed by the US government, to soft targets including schools, churches, and hospitals. Perhaps you could begin with the cross-"inspection" of security procedures by trusted colleagues from other facilities and the cross-pollination of ideas. Or, you may ask them to test your security by sending someone in to test your system. One redteaming exercise recently shared by a colleague included the "perpetrators" wearing a shirt bearing the symbol and name of a famous soft drink company. Holding a clipboard and stating the purpose was to check the soda machines, the redteamer had unlimited access to a school.

For more about the red teaming concept, please see the homepage of *The Red Team Journal,* http://redteamjournal.com/, started in 1997 by my colleague, Dr. Mark Mateski, the industry expert on the topic.

CONCLUSION

Unfortunately, the world has changed drastically since 9/11 and the places we should feel the safest and go for relaxation and recreation are in the terrorist's target book. Fortunately, other sectors such as the military provide a model for soft target hardening activities. Case studies of soft target attacks provide rich examples of successes and failures that enable you to assess your own preparation activities.

You are no longer helpless against this rising threat: you can now confidently move forward and prepare your facility, staff, and users for the unthinkable.

REFERENCES

American Red Cross. "Ready Rating Program" (http://www.readyrating.org/) (2014).

Bradley, Bud. "State of U.S. Mall Security Post 9-11" (December 17, 2013).
Butime, Herman R. "The Lay-out of Westgate Mall and Its Significance in the Westgate Mall Attack in Kenya." *Small Wars Journal* (May 10, 2014).
Canfield, Amy. "Hospital Loading Docks Rival ERs for Security Concerns." *Security Director News* (November 25, 2013).
Carpenter, Mike. "Evolving to Effects Based Operations." http://www.dodccrp.org/events/9th_ICCRTS/CD/presentations/8/092.pdf (March 2004).
City of Houston, Texas. "Run, Hide, Fight." http://www.youtube.com/watch?v=5VcSwejU2D0
DHS (Department of Homeland Security). "Active Shooter: How to Respond" (http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf) (2008).
———. "National Infrastructure Protection Plan: Commercial Facilities Sector" (http://www.dhs.gov/xlibrary/assets/nipp_commerc.pdf) n.d.
———. "Soft Target Awareness Training for Facility Managers, Supervisors, and Security and Safety Personnel: Course Syllabus" (http://www.fbiic.gov/public/2008/nov/STACsylJUL08.pdf) (2008).
FBI (Federal Bureau of Investigation). "Higher Education and National Security: The Targeting of Sensitive, Proprietary, and Classified Information on Campuses of Higher Education" (2011).
FEMA (Federal Emergency Management Agency). "Fy 2014 Urban Areas Security Initiative and Nonprofit Security Grant Program" (http://www.fema.gov/fy-2014-urban-areas-security-initiative-uasi-non-profit-security-grant-program-nsgp) (2014).
Fischbacher-Smith, Denis, and Moira Fischbacher-Smith. "The Vulnerability of Public Spaces: Challenges for UK Hospitals under the 'New' Terrorist Threat." *Public Management Review* 15, no. 3 (March 27, 2013): 330–343.
Kuhns, Kristie R., and Joseph B. Blevins. "Understanding Decisions to Burglarize from the Offender's Perspective." The University of North Carolina at Charlotte Department of Criminal Justice & Criminology (2013).
Lysiak, Matthew. *Newtown: An American Tragedy*. New York: Gallery Books, Simon and Schuster, 2013.
Marion, Steve. "Mock School Attack Tests Readiness." *The Standard Banner* (May 20, 2014).
Mateski, Mark. "Red Team Journal: Understand, Anticipate, Adapt" (http://redteamjournal.com/) (2014).
Moses, Manfred. "Synagogue Security" (2014).
National Commission on Terrorist Attacks upon the United States. (2004): 344.

Office of the State's Attorney Judicial District of Danbury. "Report of the State's Attorney for the Judicial District of Danbury on the Shootings at Sandy Hook Elementary School and 36 Yogananda Street, Newtown, Connecticut." (2013).

Rose, Roger, M., A.Vangura, Jr., and M. Levin. "Wrongful Death, Failure to Deter Crime on the Premises." *Zanin's Jury Verdict Review & Analysis* (http://www.jvra.com/verdict_trak/article.aspx?id=187168) (2009).

Sant Sipahi Advisory Team. "Security and Risk Assessment." (http://www.harisingh.com/SantSipahiAdvisoryTeam.htm)

Schrotenboer, Brent. "Holes in Stadium Security" (May 2, 2013).

Toppo, Greg. "Nerves Fray as Anniversaries of April Attacks Arrive" (April 19, 2014).

CHAPTER 10

Fifteen Takeaways about Soft Target Hardening

> Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money and national security.
>
> ***—The 9/11 Commission Report***

This book was not meant to cause panic or alarm. The purpose was to provide a compelling, data-based argument that soft targets in our country are at increased risk for attack, not only by violent criminals, but also by domestic and international terrorists. The intent was to inform about the case studies, training, education, and tools available to help you identify vulnerabilities and mitigate risk. My hope is there will be a renewed determination to take an active role in securing civilian-centric facilities and venues by community and business leaders, security sector and law enforcement personnel, and our citizens—our force multipliers. Together, we can make a difference and, I believe, save lives.

There are fifteen main takeaways that I hope you will revisit often and share in your facilities.

1. We all have a psychological blind eye to soft targeting. We cannot help it: our cultural instinct is that civilians are noncombatants and should be protected, not targeted. We do not want to think bad actors would hit our soft spot and engage where we are most vulnerable, but they will. Modern terrorism has no moral restraints.
2. Understand that soft targets are hit every day around the world. International terrorist groups are actively planning operations in the United States, but a homegrown soft target attack is more likely.

3. Know the threat in your world and in your community. Ask questions of local law enforcement; join groups such as the FBI's Infraguard or ASIS and attend chapter meetings. There may be no evidence of a threat, but that is not the same as evidence of no threat. Remember, in the "black swan" realm, what we don't know is more important than what we know.
4. Intuitively understand your vulnerabilities and how much risk you are assuming. Identify your Achilles heel as the one vulnerability that exposes you to the greatest risk and mitigate it.
5. Before investing in or relying too heavily on technology, recall a popular military axiom: "The human is the best weapon system." By honing your intuition, understanding behavioral detection tactics, and unapologetically engaging people in situations that just "don't feel right," you are taking a significant step to protect your property and its occupants. Technology should complement your other efforts, not be the central focus of your security plan.
6. Practice good steady-state leadership for outstanding crisis leadership when it is required. Frontloaded planning, training, and exercising efforts will pay dividends in an emergency situation.
7. Take steps today to harden your facility. Consider lowering the "heat" of your building by decreasing its profile, removing signage and symbols that may be inflammatory. Installing fences and raising the height on current fencing are the easiest and fastest ways to protect your property from intruders and present a fortified appearance to outsiders.
8. Consider the deterrent effect of security officers and vehicles on your property.
9. Remember, as we harden facilities, the insider threat will grow. An insider is a serious threat. An insider lone wolf is dangerous. An insider lone wolf who is a radicalized jihadist is the gravest.
10. Fight the five emotional states that increase your vulnerability: *hopelessness* (there is not much we can do to prevent or mitigate the threat), *infallibility* (it will never happen here), *inescapability* (it is destiny or unavoidable, so why even try), *invulnerability* (it cannot happen to me), and the most dangerous, *inevitability* (if it is going to happen, there is nothing I can do about it anyway).
11. When faced with a budgeting dilemma, consider this question: "What is the cost of *not* protecting our people?"
12. Focus on vulnerability, not probability.
13. Invest in preparedness, not prediction.
14. Understand that we can paint an accurate picture of consequences even if we cannot predict how likely they are to occur.

15. There is desire for balance between normalcy and vigilance. The best approach is to "bake" security fully into the culture where it permeates decision making about infrastructure and equipment purchases, event planning, and hiring and staffing activities.

Understandably, making changes for the sake of security sometimes feels like we are conceding our way of life to adversaries. Sadly, the world has changed, and so must we. Thank you for caring about and protecting our civilians from a battle they did not choose to fight.

Now is the time to convert knowledge to action.

REFERENCE

The National Commission on Terrorist Attacks upon the United States. *The 9/11 Commission Report*. 2011.

Glossary

ALF: Animal Liberation Front
AQ: Al-Qaeda
AQAP: Al-Qaeda in the Arabian Peninsula
AQI: Al-Qaeda in Iraq, now known as the Islamic State of Iraq and the Levant (ISIL or ISIS) (took advantage of instability in Syria to expand across their shared border)
AQIM: Al-Qaeda in the lands of the Islamic Maghreb
AQRO: Al-Qaeda related offense
Asymmetric operations: Using the element of surprise to attack; also, using an adversary's strength against him while exploiting his weaknesses
CBRNE: Chemical, biological, radiological, nuclear, and explosive
CTITF: Counterterrorism Implementation Task Force
DFI: Deadly force incident
DHS: Department of Homeland Security
DoD: Department of Defense
DOJ: Department of Justice
Domestic terrorism: Domestic terrorism involving groups or individuals who are based and operate entirely within the United States and US territories and whose acts are directed at elements of the US government or population (FBI)
DTEC: Domestic Terrorism Executive Committee
DTO: Drug trafficking organization
EAP: Emergency action planning
EBH: Effects-based hardening
ELF: Earth Liberation Front
FBI: Federal Bureau of Investigation
FDA: Federal Drug Administration
FEMA: Federal Emergency Management Agency
FOIA: Freedom of Information Act
FTO: Foreign terrorist organization, officially designated by the State Department
HUMINT: Human intelligence
ICT: Incident Command Team
Ideology: Visionary theorizing; a systematic body of concepts, especially about human life or culture; the manner or the content of thinking characteristic of an individual, group, or culture;

the integrated assertions, theories, and aims that constitute a sociopolitical program.

IED: Improvised explosive device

International terrorism: Terrorism involving citizens or the territory of more than one country (per 22 USCS 2656f)

INTERPOL: The organization's official name is ICPO–INTERPOL and the official abbreviation ICPO stands for International Criminal Police Organization. INTERPOL is shorthand for international police

JIEDDO: Joint Improvised Explosive Device Defeat Organization—a Department of Defense organization to defeat the IED through counter-IED (C-IED) efforts

LE: Law enforcement

LEO: Law enforcement officer

LTTE: Liberation Tigers of Tamil Eelam—a terrorist group mostly defeated in Sri Lanka in 2009

NCTC: National Counterterrorism Center

OSAC: Overseas Security Advisory Council

PPP: Public–private partnership

PVI: Place vulnerability index

Shelter in place: To stay where one is in the event of an emergency: requires people stay inside a building away from windows. If due to a biological, chemical, or radiation event, all windows and air intake systems should be closed and, if possible, covered with sheets of plastic and taped down. Wet towels may be used to seal cracks. If sheltering due to an active shooter, lock and block the door with heavy furniture. Turn off lights and silence cell phones and beepers. Text your location to someone who is outside, but insist the person not call. Get behind a turned-over desk or furniture item, in the farthest corner of the room. If sheltering due to a bomb, you must turn off all electronic devices, as many bombs are triggered by cell phones. Stay away from the windows to protect yourself from flying glass.

SSE: Sensitive site exploitation—the recovery of documents, electronic data, or other information at a sensitive location such as a war crimes site, classified facility, or the operational building or living quarters of an enemy combatant; accomplished by a specially trained team.

Tehrik-e-Taliban Pakistan (TTP): A loose alliance of militant groups in Pakistan, affiliated with the Afghani Taliban, and the force behind the failed Times Square bombing attempt

Terrorism: Premeditated, politically or religiously motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents; the unlawful use of force or

violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives

TME: Terror multiplier effect—the careful selection of targets that can reap high gains for the attacks whether through casualty counts or tactics employed

USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

VBIED: Vehicle-based improvised explosive device

WMD: Weapon of mass destruction—any explosive, incendiary, or poison gas (chemical); bomb, grenade, rocket having a propellant charge of more than 4 ounces; missile having an explosive incendiary charge of more than 0.25 ounce; mine or device similar to the above; weapon involving a disease organism (biological); or weapon that is designed to release radiation or radioactivity at a level dangerous to human life (nuclear). (Source: 18 USC 2332a as referenced in 18 USC 921)

Appendix A: List of Foreign Terrorist Organizations

United States Department of State, Bureau of Counterterrorism, June 1, 2013

Foreign terrorist organizations (FTOs) are foreign organizations that are designated by the Secretary of State in accordance with section 219 of the Immigration and Nationality Act (INA), as amended. FTO designations play a critical role in our fight against terrorism and are an effective means of curtailing support for terrorist activities and pressuring groups to get out of the terrorism business. [The first FTO designations were made on October 8, 1997.]

CURRENT LIST OF DESIGNATED FOREIGN TERRORIST ORGANIZATIONS

The list is presented in chronological order by designation; groups 1–20 were all designated on October 8, 1997.

1. Abu Nidal Organization (ANO)
2. Abu Sayyaf Group (ASG)
3. Aum Shinrikyo (AUM)
4. Basque Fatherland and Liberty (ETA)
5. Gama'a al-Islamiyya (Islamic Group) (IG)
6. HAMAS
7. Harakat ul-Mujahidin (HUM)
8. Hezbollah
9. Kahane Chai (Kach)
10. Kurdistan Workers Party (PKK) (Kongra-Gel)
11. Liberation Tigers of Tamil Eelam (LTTE)
12. National Liberation Army (ELN)
13. Palestine Liberation Front (PLF)

14. Palestinian Islamic Jihad (PIJ)
15. Popular Front for the Liberation of Palestine (PFLF)
16. PFLP-General Command (PFLP-GC)
17. Revolutionary Armed Forces of Colombia (FARC)
18. Revolutionary Organization 17 November (17N)
19. Revolutionary People's Liberation Party/Front (DHKP/C)
20. Shining Path (SL)
21. Al-Qa'ida (AQ)
22. Islamic Movement of Uzbekistan (IMU)
23. Real Irish Republican Army (RIRA)
24. Jaish-e-Mohammed (JEM)
25. Lashkar-e Tayyiba (LeT)
26. Al-Aqsa Martyrs Brigade (AAMB)
27. Asbat al-Ansar (AAA)
28. Al-Qaida in the Islamic Maghreb (AQIM)
29. Communist Party of the Philippines/New People's Army (CPP/NPA)
30. Jemaah Islamiya (JI)
31. Lashkar i Jhangvi (LJ)
32. Ansar al-Islam (AAI)
33. Continuity Irish Republican Army (CIRA)
34. Libyan Islamic Fighting Group (LIFG)
35. Islamic State of Iraq and the Levant (formerly al-Qa'ida in Iraq)
36. Islamic Jihad Union (IJU)
37. Harakat ul-Jihad-i-Islami/Bangladesh (HUJI-B)
38. Al-Shabaab
39. Revolutionary Struggle (RS)
40. Kata'ib Hizballah (KH)
41. Al-Qa'ida in the Arabian Peninsula (AQAP)
42. Harakat ul-Jihad-i-Islami (HUJI)
43. Tehrik-e Taliban Pakistan (TTP)
44. Jundallah
45. Army of Islam (AOI)
46. Indian Mujahedeen (IM)
47. Jemaah Anshorut Tauhid (JAT)
48. Abdallah Azzam Brigades (AAB)
49. Haqqani Network (HQN)
50. Ansar al-Dine (AAD)
51. Boko Haram
52. Ansaru
53. Al-Mulathamun Battalion
54. Ansar al-Shari'a in Benghazi
55. Ansar al-Shari'a in Darnah
56. Ansar al-Shari'a in Tunisia

57. Ansar Bayt al-Maqdis
58. Al-Nusrah Front (designated 5/15/2014)

Identification

The Bureau of Counterterrorism in the State Department (S/CT) continually monitors the activities of terrorist groups active around the world to identify potential targets for designation. When reviewing potential targets, S/CT looks not only at the actual terrorist attacks that a group has carried out, but also at whether the group has engaged in planning and preparations for possible future acts of terrorism or retains the capability and intent to carry out such acts.

Designation

Once a target is identified, S/CT prepares a detailed "administrative record," which is a compilation of information, typically including both classified and open sources information, demonstrating that the statutory criteria for designation have been satisfied. If the Secretary of State, in consultation with the Attorney General and the Secretary of the Treasury, decides to make the designation, Congress is notified of the Secretary's intent to designate the organization and given seven days to review the designation, as the INA requires. Upon the expiration of the seven-day waiting period and in the absence of Congressional action to block the designation, notice of the designation is published in the *Federal Register,* at which point the designation takes effect. By law an organization designated as an FTO may seek judicial review of the designation in the United States Court of Appeals for the District of Columbia Circuit not later than 30 days after the designation is published in the *Federal Register.*

Until recently the INA provided that FTOs must be redesignated every two years or the designation would lapse. Under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), however, the redesignation requirement was replaced by certain review and revocation procedures. IRTPA provides that an FTO may file a petition for revocation two years after its designation date (or in the case of redesignated FTOs, its most recent redesignation date) or two years after the determination date on its most recent petition for revocation. In order to provide a basis for revocation, the petitioning FTO must provide evidence that the circumstances forming the basis for the designation are sufficiently different as to warrant revocation. If no such review has been conducted during a five-year period with respect to a designation, then the Secretary of State is required to review the designation to determine whether revocation would be appropriate. In addition, the Secretary of State may at any time revoke a designation upon a finding that the circumstances forming the basis for the designation have changed in such a manner as to warrant revocation, or that the national security of the United States warrants a revocation. The same procedural requirements apply to revocations made by

the Secretary of State as apply to designations. A designation may be revoked by an Act of Congress, or set aside by a Court order.

Legal Criteria for Designation under Section 219 of the INA as amended

1. It must be a foreign organization.
2. The organization must *engage in terrorist activity,* as defined in section 212 (a)(3)(B) of the INA (8 U.S.C. § 1182(a)(3)(B)), or *terrorism,* as defined in section 140(d)(2) of the Foreign Relations Authorization Act, Fiscal Years 1988 and 1989 (22 U.S.C. § 2656f(d)(2)), *or retain the capability and intent to engage in terrorist activity or terrorism*.
3. The organization's terrorist activity or terrorism must threaten the security of U.S. nationals *or* the national security (national defense, foreign relations, *or* the economic interests) of the United States.

Legal Ramifications of Designation

1. It is unlawful for a person in the United States or subject to the jurisdiction of the United States to knowingly provide "material support or resources" to a designated FTO. The term "material support or resources" is defined in 18 U.S.C. § 2339A(b)(1) as "any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification, communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials." 18 U.S.C. § 2339A(b)(2) provides that for these purposes "the term 'training' means instruction or teaching designed to impart a specific skill, as opposed to general knowledge." 18 U.S.C. § 2339A(b)(3) further provides that for these purposes the term "'expert advice or assistance' means advice or assistance derived from scientific, technical or other specialized knowledge. "
2. Representatives and members of a designated FTO, if they are aliens, are inadmissible to and, in certain circumstances, removable from the United States (see 8 U.S.C. §§ 1182 (a)(3)(B)(i)(IV)-(V), 1227 (a)(1)(A)).
3. Any U.S. financial institution that becomes aware that it has possession of or control over funds in which a designated FTO or its agent has an interest must retain possession of or control over the funds and report the funds to the Office of Foreign Assets Control of the U.S. Department of the Treasury.

Other Effects of Designation

1. Supports our efforts to curb terrorism financing and to encourage other nations to do the same.
2. Stigmatizes and isolates designated terrorist organizations internationally.
3. Deters donations or contributions to and economic transactions with named organizations.
4. Heightens public awareness and knowledge of terrorist organizations.
5. Signals to other governments our concern about named organizations.

Revocations of Foreign Terrorist Organizations

The Immigration and Nationality Act sets out three possible basis [*sic*] for revoking a Foreign Terrorist Organization designation:

1. The Secretary of State must revoke a designation if the Secretary finds that the circumstances that were the basis of the designation have changed in such a manner as to warrant a revocation;
2. The Secretary of State must revoke a designation if the Secretary finds that the national security of the United States warrants a revocation;
3. The Secretary of State may revoke a designation at any time.

Any revocation shall take effect on the date specified in the revocation or upon publication in the *Federal Register* if no effective date is specified. The revocation of a designation shall not affect any action or proceeding based on conduct committed prior to the effective date of such revocation.

(From US State Department, "Foreign Terrorist Organizations." (http://www.state.gov/j/ct/rls/other/des/123085.htm)

Appendix B: NIMS, the ICS and FEMA Courses

Understanding the National Incident Management System (NIMS) is critical for leaders of soft target venues. NIMS identifies concepts and principles that answer how to manage emergencies from preparedness to recovery regardless of their cause, size, location, or complexity. NIMS provides a consistent, nationwide approach and vocabulary for multiple agencies or jurisdictions to work together to build, sustain, and deliver the core capabilities needed to achieve a secure and resilient nation. The Incident Command System (ICS) is a systematic, all-hazards tool used for the command, control, and coordination of emergency response. A terrorist attack of any kind will bring the federal government to the scene and you must understand how its representatives will operate, what they expect from you, and how you both can partner to bring the situation under control and to fruition.

The following courses provide the basis for understanding NIMS and the ICS as well as recommended FEMA online courses, available to all free of charge.

Course Code	Course Title
IS-100.b	Introduction to Incident Command System, ICS-100
IS-100.FDA	Introduction to Incident Command System (ICS100) for Food and Drug Administration
IS-100.FWa	Intro to Incident Command System (ICS100) for Federal Workers
IS-100.HCb	Introduction to the Incident Command System (ICS100) for Healthcare/Hospitals
IS-100.HE	Introduction to the Incident Command System for Higher Education
IS-100.LEb	Introduction to the Incident Command System (ICS100) for Law Enforcement
IS-100.PWb	Introduction to the Incident Command System (ICS100) for Public Works
IS-100.SCa	Introduction to the Incident Command System for Schools
IS-200.b	ICS for Single Resources and Initial Action Incidents

Course Code	Course Title
IS-200.HCa	Applying ICS to Healthcare Organizations
IS-700.a	National Incident Management System (NIMS)—An Introduction
IS-701.a	NIMS Multiagency Coordination System (MACS) Course
IS-702.a	National Incident Management System (NIMS) Public Information Systems
IS-703.a	NIMS Resource Management
IS-704	NIMS Communications and Information Management
IS-706	NIMS Intrastate Mutual Aid—An Introduction
IS-800.b	National Response Framework—An Introduction

The Professional Development Series includes seven Emergency Management Institute independent-study courses that provide a well-rounded set of fundamentals for those in the emergency management profession. After successfully completing all seven required PDS courses through the independent study program, a PDS certificate is obtained.

Course Code	Course Title
IS-120.a	An Introduction to Exercises
IS-130	Exercise Evaluation and Improvement Planning
IS-139	Exercise Design
IS-230.d	Fundamentals of Emergency Management
IS-235.b	Emergency Planning
IS-240.a	Leadership and Influence
IS-241.b	Decision Making and Problem Solving
IS-242.b	Effective Communication
IS-244.b	Developing and Managing Volunteers

Other courses by FEMA serve to educate and prepare facility leaders, operators, and security and emergency personnel on the myriad threats facing the organization. In some cases, courses may count as college credits.

Course Code	Course Title
IS-1.a	Emergency Manager: An Orientation to the Position— (2/7/2013)
IS-3	Radiological Emergency Management
IS-5.a	An Introduction to Hazardous Materials
IS-15.b	Special Events Contingency Planning for Public Safety Agencies

Course Code	Course Title
IS-22	Are You Ready? An In-depth Guide to Citizen Preparedness
IS-36	Multihazard Planning for Childcare
IS-37	Managerial Safety and Health
IS-42	Social Media in Emergency Management
IS-55.a	Household Hazardous Materials—A Guide for Citizens
IS-56	Hazardous Materials Contingency Planning
IS-75	Military Resources in Emergency Management
IS-101.c	Preparing for Federal Disaster Operations: FEMA
IS-102.c	Preparing for Federal Disaster Operations: FEMA Response Partners
IS-106.14	Workplace Violence Awareness Training 2014
IS-201	Forms Used for the Development of the Incident Action Plan
IS-208.a	State Disaster Management
IS-247.a	Integrated Public Alert and Warning System (IPAWS)
IS-248	Integrated Public Alert and Warning System (IPAWS) for the American Public
IS-271.a	Anticipating Hazardous Weather and Community Risk, 2nd edition
IS-288	The Role of Voluntary Agencies in Emergency Management
IS-301	Radiological Emergency Response
IS-315	CERT Supplemental Training: The Incident Command System
IS-318	Mitigation Planning for Local and Tribal Communities
IS-328	Plan Review for Local Mitigation Plans
IS-331	Introduction to Radiological Emergency Preparedness (REP) Exercise Evaluation
IS-340	Hazardous Materials Prevention
IS-346	An Orientation to Hazardous Materials for Medical Personnel
IS-360	Preparing for Mass Casualty Incidents: A Guide for Schools, Higher Education, and Houses of Worship
IS-362.a	Multihazard Emergency Planning for Schools
IS-366	Planning for the Needs of Children in Disasters
IS-368	Including People with Disabilities and Others with Access and Functional Needs in Disaster Operations
IS-393.a	Introduction to Hazard Mitigation
IS-394.a	Protecting Your Home or Small Business from Disaster
IS-405	Overview of Mass Care/Emergency Assistance
IS-420	Implementing the Emergency Food and Shelter National Board Program
IS-421	Overview of the Emergency Food and Shelter National Board Program

Course Code	Course Title
IS-450	Emergency Preparedness for Federal Employees
IS-450.NC	Emergency Preparedness for Federal Employees in the National Capital Region
IS-453	Introduction to Homeland Security Planning
IS-454	Fundamentals of Risk Management
IS-524	Continuity of Operations (COOP) Planner's Workshop
IS-546.a	Continuity of Operations Awareness Course
IS-547.a	Introduction to Continuity of Operations
IS-548	Continuity of Operations (COOP) Program Manager
IS-551	Devolution Planning
IS-552	The Public Works Role in Emergency Management
IS-554	Emergency Planning for Public Works
IS-556	Damage Assessment for Public Works
IS-558	Public Works and Disaster Recovery
IS-559	Local Damage Assessment
IS-660	Introduction to Public–Private Partnerships
IS-662	Improving Preparedness and Resilience through Public–Private Partnerships
IS-775	EOC Management and Operations
IS-800.b	National Response Framework, An Introduction
IS-821.a	Critical Infrastructure Support Annex
IS-836	Nuclear/Radiological Incident Annex
IS-860.b	National Infrastructure Protection Plan (NIPP)
IS-906	Workplace Security Awareness
IS-907	Active Shooter: What You Can Do
IS-908	Emergency Management for Senior Officials
IS-909	Community Preparedness: Implementing Simple Activities for Everyone
IS-910.a	Emergency Management Preparedness Fundamentals
IS-912	Retail Security Awareness: Understanding the Hidden Hazards
IS-913.a	Critical Infrastructure Security and Resilience: Achieving Results through Partnership and Collaboration
IS-914	Surveillance Awareness: What You Can Do
IS-915	Protecting Critical Infrastructure against Insider Threats
IS-921.a	Implementing Critical Infrastructure Security and Resilience
IS-2001	Threat and Hazard Identification and Risk Assessment (THIRA)
IS-2900	National Disaster Recovery Framework (NDRF) Overview

(From Federal Emergency Management Agency, http://training.fema.gov)/

Appendix C: Federal Bureau of Investigation (FBI) Terrorism Vulnerability Self-Assessment Checklist

*** WARNING: completed document must be safeguarded ***

This vulnerability self-assessment is intended to help an organization determine its vulnerability to terrorism and to assist local law enforcement in assessing the overall vulnerability of the community. It provides a worksheet that can be customized to the specific organization. The worksheet is intended to be a general guide. It may not include all issues that would be considered in every specific operation. Therefore, it is imperative to consider the unique character of the organization: its functions, its general public image, and its overall public visibility. Consider both who may work in the organization and what the organization does. Assess the symbolic value of the organization to the public. Each worksheet section is ranked on a twenty-point scale. Answering this self-assessment is a subjective process. The person who best knows the physical security and community value of the organization should complete the worksheet. There are no firm guidelines on how to score a category. Because the questions are subjective, give a best estimate when scoring each question.

It is important to remember that the most important threat reduction measure is vigilance on the part of the organization's staff, their awareness of anything out of the ordinary, and their prompt communication of that information to the organization's security team or management. This assessment follows exactly the same format as the community assessment performed by local law enforcement to assist in preventing criminal acts committed by terrorists. Based on the results of this assessment, the organization may wish to share a copy with law enforcement, or to include their representative in the assessment process,

to support their understanding of the transportation function and its role in the community.

This assessment should be conducted at least annually, and within the year if there is an increased threat of a terrorist event or whenever there is a significant change to the organization's facilities or activities.

Upon receipt of a high-risk assessment, each law enforcement agency sheriff, chief of police, head, or his or her designated representative may forward that assessment, or other threat report, to the state emergency management agency (or equivalent), to state law enforcement, or to the local FBI office.

Vulnerability self-assessments completed by or provided to state or local governments will be used to prevent crime and may be exempt from disclosure under the public records law; check with your local law enforcement office for clarification. Threat vulnerability self-assessments in the possession of private organizations are not public records. Completed terrorism vulnerability self-assessments should be provided to local law enforcement in hard copy or on digital media. They should not be e-mailed.

Facility name:
Facility type:
Facility owner—name/cell #:
Facility point of contact for emergency response—name/cell#:

Please provide the latitude, longitude, and elevation of the main entrance to your facility. If you do not have access to a GPS unit, please contact your local law enforcement office for assistance.

_____ Lat/Long/Elevation

THE ASSESSMENT

This assessment checklist is broken down into seventeen different categories as follows:

1. Potential terrorist intensions
2. Specific targeting
3. Visibility of your facility or system within the community
4. On-site hazards
5. Population of sites, facility, or activity
6. Potential for mass casualties
7. Security environment and overall vulnerability to an attack

8. Critical products or services
9. High-risk personnel
10. Organization communication systems
11. Security and response
12. Policies, procedures, and plans
13. Security equipment
14. Computer securities, cyber crime, and cyber terrorism
15. Suspicious mail and packages
16. Telephone, bomb, and other types of threats
17. Employee health and the potential for bioterrorism

To complete the assessment, circle the evaluated score on each scale for each question. Then total the scores and enter the total on the last page. Based on the total, use the score guide to assign an overall ranking to the transportation organization.

1. Potential terrorist intentions

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Are you aware of any terrorist threat to your organization?
- Are you aware of a history of terrorist activity in your area or your specialty?
- Are you aware of the level of capability of any suspected terrorist that you believe poses a threat to your organization?

2. Specific targeting

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Have you obtained current information from law enforcement or other sources that terrorists have targeted your organization?
- What is the reliability of these information sources?
- What is your organization's public visibility?
- Does the nature of your organization's activity lead you to think it may be targeted?
- Are there activities that indicate possible terrorist preparations in your area or specialty?

3. Visibility of your facility or activity within the community

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Is your organization well known in the community?
- Do you regularly receive media attention?
- Is your organization nationally prominent in your field or industry?
- Are your location and the nature of your activity known generally to the public?
- Have you ever had an event or accident with potential health risks that attracted public attention to your facility?

4. On-site hazards

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Are hazardous materials, explosives or other dangerous items on your site?
- Do you store or use biologic or chemical materials that have the potential to be used as a threat or weapon?
- Do you store or use radioactive material at your site?
- Do you have a system to control access to hazardous materials, explosives or any other dangerous materials at your site?
- Can any products stored or used on your site be used as or in the manufacture of a mass casualty weapon?
- Can any products stored or used on your site cause extensive environmental damage?

5. Population of site, facility, or activity

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do you have more than 250 people normally present at your site?
- Do you have more than 1,000 people normally present at your site?
- Do you have more than 5,000 people normally present at your site?
- Do you hold events at your site that attract large crowds?

6. Potential for mass casualties

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do materials stored or used at your site have the potential to create mass casualties on-site?
- Do materials stored or used at your site have the potential to create mass casualties within 1 mile of your site?
- How many people live or work within 1 mile of your site? 500? 1,000? 2,000? 5,000? More than 5,000?

7. Security environments and overall vulnerability to an attack

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Does your organization have effective internal security procedures?
- What is the law enforcement presence in your area?
- What is the hardness, level of blast protection, etc. of your facilities?
- How accessible (security presence, access control, id badges, metal detection buffer zones, fences, etc.) is your facility?
- Are your assets and/or their potential recognized as a symbol?
- What level of public access is necessary for you to function?
- Can you control high-speed vehicle approaches to your facility?
- Do you have access control to your parking area?
- Do you conduct vehicle searches when entering facility grounds or parking areas?
- Do you employ detection/monitoring systems (video surveillance, intrusion detection systems, etc.)?
- Is your parking delivery area adjacent to or near your facility?
- Is your delivery area supervised during hours of normal business?
- Is your delivery area access blocked during hours that your business is closed?
- Do you have an on-site food service facility for employees and visitors?
- Is access to the water supply for your facility protected?
- Is access to the ventilation system for your facility protected?
- Do you have a way to shut down the water supply or ventilation system for your facility quickly?

8. Critical products or services

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- What is the importance of your organization to the community?
- Is your organization critical to the local population, economy, or government?
- Is your organization critical to the continuity of basic services?
- Is your organization critical to state or national commerce?
- What would be the social, economic, or psychological ramifications of a terrorist attack against your organization?
- What is the nature of your assets: hazardous materials, uniqueness, potential danger to others, etc.?
- How long would it take to restore your critical services/functions?

9. High-risk personnel

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do you have personnel that are critical to the continuing function of state or local government, basic services, utilities infrastructure, the community, the economy, or of inherent value to your business or agency?
- Do you have personnel that are critical for responding to a terrorist act?
- What would be the effect of a terrorist act against these high-risk personnel?

10. Organization communications

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do you have a mass notification system (public address system, intercoms, and alarms)?
- Do you have a secure communications network that can be relied upon during a crisis?
- Do you have a crisis response team?

- Is your crisis response team trained?
- Do you conduct regular exercises?
- Do local/regional emergency responders participate in your exercises?
- Does your crisis response team have its own portable communications system?
- Can your crisis response team communicate directly with emergency responders?
- Do you have an emergency law enforcement notification system such as a hotline, panic button, or something similar?
- Is your alarm system tied into the local law enforcement department or do you have an alarm service?
- Are your systems tested regularly?

11. Securities and response

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Are your security forces' staffing and training levels adequate?
- Do you have the capability to maintain a security presence in a high-threat situation?
- Are additional security personnel available if requested?
- Are there affiliated agency/industry/organization support services available?
- Do you have trained disaster response teams within the organization?
- Do you have necessary specialty detection, monitoring, hazard assessment devices on hand and are they functional?
- Are local/regional law enforcement forces adequate and can they respond rapidly?
- Are local emergency responders familiar with your facility and its contents?
- Do you keep records on who visits your facility and where they go within the facility?

12. Policies, procedures, and plans

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do you have a current crisis response/disaster plan?

- Does your plan include the types of crises you are most likely to encounter (e.g., fire, explosion, chemical release)?
- Are your employees familiar with the plan?
- Have you conducted crisis response and disaster drills and were they effective?
- Have you identified the critical functions of your workplace and do you have a plan for continuation of operation during an emergency?

13. Security equipment

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do you have a security system and is it current technology?
- Do you have an intrusion monitoring motion detector or an alarm system?
- Do your systems have backup if power is cut or fails?
- Do you have security equipment that would detect leaks or ruptures of potentially hazardous materials?
- Do you have personnel protective equipment for your emergency response team appropriate for the hazardous materials at your facility?
- Is such equipment in working order and has it been inspected recently?

14. Computer securities, cyber-crime, and cyber-terrorism

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Is your site dependent on information technology such as computers and networks to accomplish its daily business activities?
- Is the information stored in your computer systems valuable?
- Do you have backup power available for your computer systems?
- Do you make backup copies of your data?
- Is your backup data securely stored?
- Does your site have computers or networks connected to the Internet?
- Have you experienced problems with computer security incidents, such as computer viruses, worms, website defacements, and/or denial of service attacks in the past?

- Do you have staff in place who are adequately trained and are available to monitor security warnings and take protective measures, such as loading system patches?
- Do you have technology security tools in place such as firewalls, intrusion detection systems, or antivirus software to protect your computer systems?
- Do you have a computer security policy, plan, and procedure that include a computer security incident response team?

15. Suspicious mail and packages

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Is the mail for your facility opened in a secured area or an area isolated from the majority of personnel?
- Have the personnel who open mail received training on the recognition of suspicious mail and/or packages?
- Do you have specific procedures on how to handle suspicious mail and/or packages, including possible facility evacuation?
- Do you have a secure and contained location where any unusual or suspect deliveries or mail can be stored until proper authorities can evaluate the suspect items?

16. Telephone, bomb, and other types of threats

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Has your staff received training on how to handle bomb and other threat calls?
- Does your staff have a checklist of questions to ask the caller in case of a bomb or other threatening call?
- Does your facility have a plan on how to handle bomb and other threatening calls?
- Does your bomb threat plan include a system whereby your personnel would search your facility to identify suspicious objects to point out to emergency response personnel?
- Does your plan include a decision-making process on whether to evacuate the facility?
- Are personnel familiar with the plan? Have evacuation drills been conducted?

- Is your plan coordinated with local law enforcement and the local phone company?

17. Employee health and the potential for bioterrorism

Low Vulnerability										High Vulnerability									
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20

The following are issues to be considered in selecting your score.

- Do you have an occupational health safety program in place?
- Do you have a health professional working at your facility?
- Do you have a procedure in place to track the health of each employee and know if more than one employee has the same symptoms?
- Do you monitor the health status of employees on sick status or absent otherwise?
- Are employees encouraged to keep supervisors informed on any unusual health-related event or condition?
- Are employees required to report any unusual conditions or substances encountered in the course of their normal duties, such as strange substances or odors from packaging or mail?
- Do employees know the proper procedures for emergency operation or shut-off of air handler, air-circulating, or ventilation systems?
- Do you keep a current list of employees and their home addresses and emergency contact information?
- Do you have an emergency notification plan for employees (e.g., calling tree)?

Total score: _____	
Self-Assessment Evaluation	
(20–85)	**Low risk**
(86-170)	**Low caution**
(171–225)	**High caution**
(256–340)	**High risk**

If the total score for the organization exceeds 256 and if local law enforcement has not been involved in the assessment, notify them at once. Again, hand carry and do not e-mail or mail the document.

Remarks and Unusual or Significant Issues

Please list any important remarks that should be made concerning the self-assessment. Also, please list any unusual or significant findings that developed during your self-assessment. List significant hazardous materials that might be used as a terrorist weapon or any significant impact a terrorist act against your site may cause to the community.

Notes:

*** WARNING: Completed Document Must Be Safeguarded ***

(From "Federal Bureau of Investigation Vulnerability Self-Assessment." http://globalsecurityplanning.com/vulnerability-assessments/fbi-vulnerability-self-assessment)

Appendix D: Bomb Threat Checklist

(For placement next to every telephone in the organization.)

BOMB THREAT CALL PROCEDURES

Most bomb threats are received by phone. Bomb threats are serious until proven otherwise. Act quickly, but remain calm and obtain information with the checklist on the reverse of this card.

If a bomb threat is received by phone:

1. Remain calm. Keep the caller on the line for as long as possible. DO NOT HANG UP, even if the caller does.
2. Listen carefully. Be polite and show interest.
3. Try to keep the caller talking to learn more information.
4. If possible, write a note to a colleague to call the authorities or, as soon as the caller hangs up, immediately notify them yourself.
5. If your phone has a display, copy the number and/or letters on the window display.
6. Complete the Bomb Threat Checklist (reverse side) immediately. Write down as much detail as you can remember. Try to get exact words.
7. Immediately upon termination of the call, do not hang up, but from a different phone, contact FPS immediately with information and await instructions.

If a bomb threat is received by handwritten note:

- Call _____
- Handle note as minimally as possible.

If a bomb threat is received by email:

- Call _____
- Do not delete the message.

Signs of a suspicious package:

- No return address
- Excessive postage
- Stains
- Strange odor
- Strange sounds
- Unexpected delivery
- Poorly handwritten
- Misspelled words
- Incorrect titles
- Foreign postage
- Restrictive notes

DO NOT:

- Use two-way radios or cellular phone; radio signals have the potential to detonate a bomb.
- Evacuate the building until police arrive and evaluate the threat.
- Activate the fire alarm.
- Touch or move a suspicious package.

WHO TO CONTACT (select one)

- Follow your local guidelines
- Federal Protective Service (FPS) Police
  1-877-4-FPS-411 (1-877-437-7411)
- 911

BOMB THREAT CHECKLIST

Date: ☐ **Time:** ☐

Time Caller Hung Up: ☐ **Phone Number Where Call Received:** ☐

Ask Caller:

- Where is the bomb located? (Building, Floor, Room, etc.)
- When will it go off?
- What does it look like?
- What kind of bomb is it?
- What will make it explode?
- Did you place the bomb? Yes No
- Why?
- What is your name?

Exact Words of Threat:

Information About Caller:

- Where is the caller located? (Background and level of noise)
- Estimated age:
- Is voice familiar? If so, who does it sound like?
- Other points:

Caller's Voice

- ☐ Accent
- ☐ Angry
- ☐ Calm
- ☐ Clearing throat
- ☐ Coughing
- ☐ Cracking voice
- ☐ Crying
- ☐ Deep
- ☐ Deep breathing
- ☐ Disguised
- ☐ Distinct
- ☐ Exited
- ☐ **Female**
- ☐ Laughter
- ☐ Lisp
- ☐ Loud
- ☐ **Male**
- ☐ Nasal
- ☐ Normal
- ☐ Ragged
- ☐ Rapid
- ☐ Raspy
- ☐ Slow
- ☐ Slurred
- ☐ Soft
- ☐ Stutter

Background Sounds:

- ☐ Animal Noises
- ☐ House Noises
- ☐ Kitchen Noises
- ☐ Street Noises
- ☐ Booth
- ☐ PA system
- ☐ Conversation
- ☐ Music
- ☐ Motor
- ☐ Clear
- ☐ Static
- ☐ Office machinery
- ☐ Factory machinery
- ☐ Local
- ☐ Long distance

Other Information:

Threat Language:

- ☐ Incoherent
- ☐ Message read
- ☐ Taped
- ☐ Irrational
- ☐ Profane
- ☐ Well-spoken

Homeland Security

FIGURE D1 Department of Homeland Security bomb threat checklist.

Appendix E: National Counterterrorism Center Bomb Threat Standoff Charts

(Map your property and the surrounding area with these evacuation distances.)

	Explosives Capacity[1] (TNT Equivalent)	Mandatory Evacuation Distance[2]	Preferred Evacuation Distance[3]
Pipe bomb	5 LBS/2.3 KG	70 FT/21 M	1,200 FT/366 M
Suicide vest	20 LBS/9.2 KG	110 FT/34 M	1,750 FT/518 M
Briefcase/suitcase bomb	50 LBS/23 KG	150 FT/46 M	1,850 FT/564 M
Sedan	500 LBS/227 KG	320 FT/98 M	1,900 FT/580 M
SUV/van	1,000 LBS/454 KG	400 FT/122 M	2,400 FT/732 M
Small delivery truck	4,000 LBS/1,814 KG	640 FT/195 M	3,800 FT/1159 M
Container/water truck	10,000 LBS/4,536 KG	860 FT/263 M	5,100 FT/1,555 M
Semi-trailer	60,000 LBS/27,216 KG	1,570 FT/479 M	9,300 FT/2,835 M

FIGURE E1 National Counterterrorism Center bomb threat standoff chart. (1) Based on maximum volume or weight of explosive (TNT equivalent) that could reasonably fit in a suitcase or vehicle. (2) Governed by the ability of typical US commercial construction to resist severe damage or collapse following a blast. Performances can vary significantly, however, and buildings should be analyzed by qualified parties when possible. (3) Governed by the greater of fragment throw distance or glass breakage/falling glass hazard distance. Note that pipe and briefcase bombs assume cased charges that throw fragments farther than vehicle bombs. (4) A known terrorist tactic is to attract bystanders to windows, doorways, and the outside with gunfire, small bombs, or other methods and then detonate a larger, more destructive device, significantly increasing human casualties.

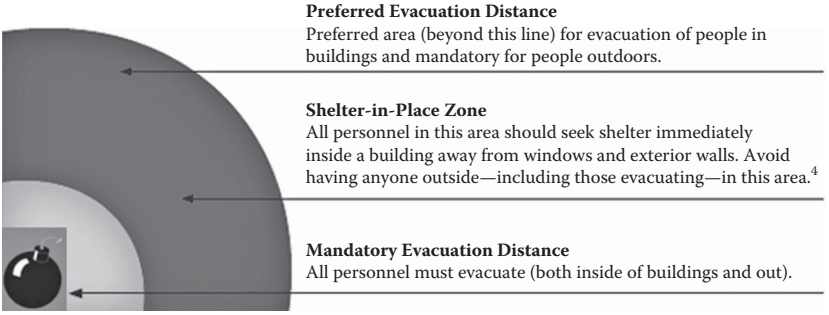

Preferred Evacuation Distance
Preferred area (beyond this line) for evacuation of people in buildings and mandatory for people outdoors.
Shelter-in-Place Zone
All personnel in this area should seek shelter immediately inside a building away from windows and exterior walls. Avoid having anyone outside—including those evacuating—in this area.[4]
Mandatory Evacuation Distance
All personnel must evacuate (both inside of buildings and out).

FIGURE E2 National Counterterrorism Center bomb shelter in place and evacuation chart.

Appendix F: Planning and Emergency Smartphone Applications

During the violent earthquake in Haiti, a victim trapped in the rubble used his iPhone app to save his life. Trapped for 65 hours in the lobby of his Port-au-Prince hotel, Dan Woolley used information from an iPhone first-aid app to make a tourniquet for his fractured leg and stanch the bleeding from his head wound. He also used his camera to take pictures of his wounds so that he could zoom in and assess the extent of the injuries (Katz 2010). At the very least, there is a psychological aspect to victims participating in self-care and taking control instead of feeling panic or loss of determination, especially for those who are trapped alone and isolated.

The following list of applications is not all inclusive, but rather a few recommended for the book by law enforcement, first responders, and emergency response experts:

911 toolkit
Bomb threat standoff
Close call
Compass
CPR and choking
Emergency radio (scanner)
Emergency response guidebook
Emergency survival handbook
First aid by American Red Cross
Flashlight with SOS and beacons
GPS
HazMat reference
iPhone tracking
iStethoscope
iTriage
Mobile REMM
palmEM emergency medicine

Pocket first aid
Police siren (possibly use to scare away intruders)
Radar scope—weather app
Wiser—HazMat app

Companies are also developing apps that users can purchase to access password-protected information and secretly communicate. For example, Spot-on Response provides vital information to emergency responders including blueprints and building evacuation plans. The app also allows for silent, two-way communication; for instance, teachers can use the app to discreetly send a message to notify first responders of their location and also send pictures of the scene to assist in recovery operations. The Nordonia Hills school district in northeastern Ohio was one of the first to use Spot-On Response to enhance school safety (Simmons 2014).

REFERENCES

Katz, Leslie. "iPhone App Helped U.S. Man Survive Haiti Quake." (January 10, 2010).
Simmons, Brandon. "Technology Can Help School Attack Response." (April 9, 2014).

Appendix G: Primary and Secondary School Threat Assessment and Response Checklist

Although the size and scope of an attack on our education system the scale of a Beslan-style attack seems unlikely, we still are susceptible to international or domestic terrorist activity. The school may be colocated with a hard target, such as a military installation, or be caught up in a large-scale attack, such as the schools in Manhattan on 9/11. The school district should take a leadership role and clearly state its goals along with outcome-based, measurable objectives for the program that reflect the intent of the program and address the major aspects of its purpose. The following checklist is not meant to be all inclusive and serves as a basis for planning; your checklist should be tailored to your unique organization and situation.

THREAT ASSESSMENT

With any emergency action planning (EAP) activity, response to a terrorist event should be an annex added to existing plans. For example, a terrorist attack differs from the active-shooter scenario in many ways, so do not try to cover both events with the same checklist. An active shooter is defined as

> …an individual actively engaged in killing or attempting to kill people in a confined and populated area; in most cases, active shooters use firearms(s) and there is no pattern or method to their selection of victims. Active shooter situations are unpredictable and evolve quickly. Typically, the immediate deployment of law enforcement is required to stop the shooting and mitigate harm to victims. Because active shooter situations are often over within 10 to 15 minutes, before law enforce-

> ment arrives on the scene, individuals must be prepared both mentally and physically to deal with an active shooter situation. (DHS 2008)

Whereas most active-shooter incidents evolve and resolve themselves relatively quickly, terrorists typically seek the prolonged spectacle of media, first responder, and public response, thus gaining exposure for their cause and legitimacy. Where active-shooter incidents are not as well planned, terror actions could be planned for weeks, months, or even years before the actual incident unfolds. Furthermore, active-shooter incidents are typically perpetrated by either disgruntled employees or students who usually have minimal weapons training and bring rudimentary explosives to the scene. However, terrorists have characteristically received some form of paramilitary/insurgency training, may have a greater depth of understanding in explosives and construction of improvised explosive devices, and have access to larger financial support networks to acquire superior materials.

Although you may certainly use another organization's EAP as a model for yours, tailor the response to your unique situation and challenges.

PLANNING THE ANTI- OR COUNTERTERRORISM ANNEX TO YOUR SCHOOL EMERGENCY RESPONSE PLAN

The threat assessment and planning team should consist of, as a minimum:

- The district superintendent
- Respective district principals
- District resource officer or, in the case of larger districts, the district police chief
- Transportation director
- Facilities director
- Local law enforcement liaison
- Local fire department liaison
- Local emergency medical liaison
- Local "first care hospital" liaison

When planning your terror threat assessment, the team must consider any and all terrorist attack scenarios that might affect the school. A good question to consider is: Are other potential terror targets near the school?

- Military facility (including recruiting stations)
- Federal, state, or local governmental offices (include any and all, no matter how small the operation)

- Nuclear power plant
- Airport, train station, bus station
- Mall or outdoor shopping area
- Location in an area known for militia, sovereign citizen, or other antigovernment activities
- What is the demographic constitution of your student body and how could it be the target of a racial, religious, or other attack?

As discussed in Chapter 8, employee screening is critical because the insider threat is significant and rising. A few suggestions include:

- Review employment screening policy and procedure (administration officials)
  - Does your screening process include volunteers, cafeteria workers, mechanics, bus drivers, and security, in addition to educational staff?
  - Does your procedure allow for actual courthouse document searches, rather than online Internet database searches, which are usually not as accurate?
  - Do your searchers run Social Security number traces to identify any out-of-state issues that should be checked?
  - Do your outside contractors and their potential subcontractors use due-diligence screening procedures to check the backgrounds of their workers who regularly visit your school?
- Review the physical security of bus yards and garages; review transportation security in general (security, bus garage manager, and administration officials)
  - Are vehicle garages alarmed, and are the alarms in working order?
  - Are fenced-in areas gated, locked, and adequately illuminated at night?
  - Do drivers accomplish "pilot inspections" of their vehicles before placing them into service each day?
    - Perform rear to front inspections, both left and right sides and on board the bus itself, looking for signs of tampering, hanging wires, suspect conditions.
    - Redo inspection after the vehicle has been left unattended.
  - Are bus drivers equipped with two-way radios or cell phones?
  - Are drivers trained to be aware of and report suspicious vehicles that appear to be following their buses during their routes?
  - Do drivers keep a student roster for each bus route, to include student name, address, primary and secondary emergency contact numbers, and medical authorization information (if allowed by state law)?

- Review the adequacy of physical security in and around campus buildings (security and administration officials)
  - Are alarm systems working and have they been tested on a regular basis? This should include main campus buildings as well as maintenance and storage facilities.
  - Are keys to campus and administration buildings adequately controlled?
  - Are alarm pass codes changed when an employee leaves the school? Also, make sure that codes are not widely shared and not a typical sequence (e.g., 1-2-3-4).
  - Is exterior lighting working and is illumination adequate?
  - Is interior lighting (night lighting) working and is illumination adequate?
- Review access control procedures and heighten employee awareness (security and administration officials)
  - Are doors that should remain locked from the outside during the day kept locked, and are these doors checked periodically to make sure that they are secure?
    - Train all employees to check these doors, but also consider assigning someone the duty.
  - Are staff members trained to approach and to assist/screen strangers of any age who are observed in and on school property?
    - Immediately report those who have difficulty explaining their presence.
    - Have a visitor log and ID badge system been implemented?
  - Train everyone to recognize and report suspicious activities on campuses (all staff and students, security and administration officials)
  - Are observers who are taking pictures or filming campus activities questioned about their authorization to do so?
  - Be alert for suspicious vehicles that seem to have no apparent purpose for being on campus or that come, go, and then reappear.
  - Are specific individuals assigned to inspect the outside of campus buildings throughout the day and to report unattended packages or vehicles near building perimeters?
    - Have you developed a plan to handle reports of suspicious activity?
    - Is everyone trained to report unattended or otherwise suspicious packages found inside campus buildings? Is this specific issue placed on routine checklists for maintenance and janitorial personnel?

    - Do personnel know what to do if a suspicious package is found?
    - Have you considered a policy that requires staff and students to identify backpacks, book bags, briefcases, and gym bags visibly with luggage style ID tags?
- Do you conduct enhanced threat assessments on anniversaries of terror or antigovernmental attacks/activities (security and administration officials)?
    - February 28, start of the Waco Branch Davidian siege
    - March 19, US Invasion of Iraq
    - April 19, Oklahoma City bombing; end of the Branch Davidian siege
    - April 20, Columbine school shooting
    - May 2, death of Osama Bin Laden
    - September 11, attacks on the World Trade Center and Pentagon
    - September 1, Beslan school siege
    - October 7, US invasion of Afghanistan

These are just a few examples of international and domestic terror/US military combat events that could trigger an attack. Take into consideration your own local anniversaries that could represent a "day of remembrance" to local groups.

- Implement a "tip line" program that allows students, teachers, parents, staff, and other members of the school community to report security-related concerns anonymously, if they choose
    - Do you have a zero tolerance for verbal/physical threats of any kind?
    - Do all members of the school community know that any threat or information about a potential threat must be reported?
    - Do students and staff know that they are responsible for informing the building principal about any information or knowledge of a possible or actual terrorist threat or violent criminal act?
    - Have you communicated a hard stand on hoaxes intended to mimic terrorist acts?
    - Do students understand that these hoaxes are crimes in themselves?
- Train staff on identifying and handling suspicious packages and letters (security and administration officials)
    - Look for any of the following:
        - If delivered by carrier, check balance to see if parcel is lopsided or heavy sided.

  - Handwritten addresses or labels from companies are improper; contact the company and, if it exists, see if it sent a package or letter.
  - Packages wrapped in string are automatically suspicious, as they cannot go through the mail system.
  - Excess postage on small packages or letters indicates that the object was not weighed by a post office.
  - Be aware of no postage or noncanceled postage.
  - Be aware of any foreign writing, addresses, or postage.
  - Watch for handwritten notes, such as "To Be Opened in the Privacy of…", "CONFIDENTIAL," etc.
  - Note improper spelling of common names, places, or titles.
  - Look for generic or incorrect titles.
  - Be aware of leaks, stains, powder or protruding wires, string, tape.
  - Watch for hand delivered or "dropped off for a friend" packages or letters.
  - Look for no return address or nonsensical return address.
- Note any letters or packages arriving before or after a phone call from an unknown person asking if the item was received.

Remember that most package bombs are delivered and set up by the attacker.

- Train staff on identifying and handling bomb threats (security and administration officials)
  - Does every phone have the bomb threat checklist (see Appendix D) located nearby?
  - Have all staff members handling phone calls been instructed on its use and importance?
  - Have staff members been trained on bomb threat procedures? If a suspected package is found:
    - Do not use cell phones or two-way radios.
    - Do not move or touch a suspected package.
    - Do not activate the fire alarm.
    - Have designated search teams been identified?
      - In some cases local police bomb squads may require that staff members assist in the search, as they have intimate knowledge of the building and its contents
  - Have staff been instructed on search patterns for rooms?
    - Search with at least two people per room.

  - Divide the room into equal parts, preferably down the middle.
  - First, search from floor to waist level.
  - Second, search waist level to top of the head.
  - Third, search head to ceiling.
  - Fourth, look into the false ceilings.
  - Search points:
    - HVAC ducting
    - Rooftops
    - Window ledges
    - Bushes
    - Garbage cans
    - Flower arrangements
    - Air conditioner units
    - Automobiles
- Has an emergency response team (ERT) been delegated and trained? It can be modeled after FEMA's community emergency response team (CERT) concept. Depending on your student population, the size of this team should be between 7 and 12 individuals.
- Has the ERT been trained on the use of the incident command system and adapted its principles for use in an education setting?
- Has an incident command team been delegated with, at the minimum, the following positions:
  - The incident commander has overall command and control responsibility for the incident.
  - The operations leader leads the ERT.
  - The public information officer works closely with the incident commander, the building principal, and the district superintendent to keep media and parents informed as the incident situation develops.
  - The liaison officer works closely with the incident commander and the local first responders in the relay of information regarding operations and response.
- The safety officer works closely with the incident commander, operations leader, and the liaison officer in ensuring safe conduct of any and all responses.

At some point during the incident the local first responders will assume control; however, do not disband your incident command team until after the incident has concluded. The incident command team should stay activated even during the recovery phase of the operation.

EXERCISE THE PLAN

- Have staff trained with local first responders?
- Have full-scale exercises with staff and first responders been conducted at least once a year?
- Have table-top exercises been conducted quarterly?
- Has consideration been given to conduct full-scale exercises with students and staff present to add to realism of response and challenges?
- Have threat briefings been administered to staff on a regular basis (recommend at least once a year)?

EVALUATE THE PLAN AND EXERCISE

Once the planning and exercises are complete, conduct an after-action review to discuss areas of weakness, such as:

- What was effective with your communication laydown and what were the challenges?
- Does the plan allow for flexibility of initiative at the scene?
- Is the plan "built to fit the situation" or does the situation drive the plan?
- Did first responders and school officials understand their roles and responsibilities?
- Was an outside or an in-house evaluator used? How did this impact the assessment?
- If changes to the plan are necessary, have deadlines been established for their completion?

FINAL THOUGHTS

Leadership is key to all emergency planning and response actions. If you are not the top decision maker in your organization, you must have your leadership's buy-in; without it, your plan is nothing more than words on paper. You also must be a strong advocate for security in your organization, even if others call you a maverick or approach the topic with a sense of infallibility: it has never happened before; therefore, it will not happen. Certainly the Beslan School never saw what was coming, nor did any of the schools involved in violent crimes in our country. At the very least, preparing for a prolonged, intense terrorist attack will enable you and your staff to handle minor issues with ease.

The world has changed over the last decade—more than any one of us could have imagined. Thirty years ago, the only emergency-related thing we had to worry about at school was the surprise annual fire drill. The escalating violence in our world and attacks on soft targets such as schools, churches, and hospitals have taught us that we are no longer safe in those places we once considered protected sanctuaries. We must strive to provide a safe environment for our innocent citizens, especially our nation's children and those who wake every day to perform one of the most noble of professions, teaching.

(With thanks to Mr. Ralph Fisk (2014), emergency response and risk management expert.)

REFERENCES

FEMA (Federal Emergency Management Agency). "Community Emergency Response Teams." (http://www.fema.gov/community-emergency-response-teams).

Fisk, Ralph R., Jr. Fisk Consultants blog. (https://fiskconsultants.wordpress.com/) (2014).

DHS (Department of Homeland Security). http://www.dhs.gov/xlibrary/assets/active_shooter_booklet.pdf (2008).

HOMELAND SECURITY

Soft Target Hardening

Protecting People from Attack

Terrorist attacks occur daily and are increasingly being aimed at civilian populations around the world. Battlefield lines have been redrawn to include churches, schools, hospitals, and malls. This breach of moral boundary is shocking and invokes fear—two primary goals of terrorism.

Although there is an increase in soft target activity—or attacks on places of worship, study, and leisure—there is hesitation to explore such susceptibility in the United States. ***Soft Target Hardening: Protecting People from Attack*** starts the national dialogue by providing case studies, best practices, and methodologies for identifying soft target vulnerabilities and reducing risk in the US. Offering deterrence and mitigation techniques from more than 275 sources, this comprehensive book:

- Explores US cultural nuances contributing to the country turning a psychological blind eye toward soft target threats
- Assesses the attractiveness of soft target threats presented by foreign and domestic terror groups and drug trafficking organizations
- Analyzes the unique vulnerabilities of churches, schools, hospitals, malls, sporting and recreational events, and other soft targets
- Gives an overview of soft target hardening tactics from global hotspots, including first-person accounts and photographs
- Introduces the concept of effects-based hardening, derived from the military model of effects-based operations
- Discusses emerging soft target challenges such as insider threats, kidnapping, and use of human shields
- Evaluates the likelihood of the use of weapons of mass destruction against civilian-centric venues

Soft Target Hardening: Protecting People from Attack is a must read for those who secure, own, and operate soft target facilities, and for citizens who want to protect themselves and their families from attack.

Cover photo credits:
Cathedral of Bamberg, Bavaria: Andreas Zerndl
Loma Linda University Medical Center: Lowe R. Llaguno

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK

K23472

ISBN: 978-1-4822-4421-2
90000
9 781482 244212

www.crcpress.com